U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.2	NRC CLASSIFIED INFORMATION SECURITY PROGRAM	DT-17-226
Volume 12	Security	
Approved By:	Mark A. Satorius Executive Director for Operations	
Date Approved:	June 25, 2014	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of Nuclear Security and Incident Response Division of Security Operations	
Contact Name:	Krista Ziebell 301-415-7121	Robert Norman 301-415-2278

EXECUTIVE SUMMARY

Directive and Handbook 12.2 are revised to incorporate new requirements of—

- Executive Order 13526, "Classified National Security Information," dated December 29, 2009;
- COMSECY-04-0006, "Proposed Staff Discussions of Classified Information with the British, February 26-27, 2004," dated February 13, 2004;
- COMSECY-04-0034, "Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated June 14, 2004;
- COMSECY-10-0006, "Proposed Exchange of Classified and Safeguards Information with the United Kingdom – September 2010," dated June 8, 2010, and the associated Staff Requirements Memorandum; and
- Other NRC policy changes that are related to information security requirements.

In addition, this revision incorporates recommended changes resulting from the Office of the Inspector General Audit 13-A-21, "Audit of NRC's Implementation of Federal Classified Information Laws and Policies," dated September 12, 2013, regarding the training requirements for original and derivative classification authorities, and classified information self-inspections.

TABLE OF CONTENTS

I. POLICY....2
II. OBJECTIVE....3
III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY....3
A. Chairman....3
B. Commission....3
C. Executive Director for Operations (EDO)....3
D. Deputy Executive Director for Reactor and Preparedness Programs (DEDR)....4
E. Deputy Executive Director for Corporate Management (DEDCM)....5
F. Inspector General (IG)....5
G. Office of the General Counsel (OGC)....5
H. Director, Office of International Programs (OIP)....6
I. Secretary of the Commission (SECY)....6
J. Director, Office of Nuclear Security and Incident Response (NSIR)....6
K. Director, Division of Security Operations (DSO), NSIR....6
L. Director, Office of Nuclear Material Safety and Safeguards (NMSS)....7
M. Director, Office of Information Services (OIS)....7
N. Director, Computer Security Office (CSO)....7
O. Office Directors and Regional Administrators....7
P. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)....8
IV. APPLICABILITY....8
V. DIRECTIVE HANDBOOK....9
VI. EXCEPTIONS OR DEVIATIONS....9
VII. REFERENCES....9

I. POLICY

It is the policy of the U.S. Nuclear Regulatory Commission to ensure that classified information is handled appropriately and is protected from unauthorized disclosure in accordance with the Atomic Energy Act (AEA) of 1954, as amended; the Energy Reorganization Act of 1974, as amended; Public Law 111-258, “Reducing Over-Classification Act”; Executive Orders (E.O.) (e.g., E.O. 12829, “National Industrial Security

Program"; E.O. 12968, "Access to Classified Information"; E.O. 13526, "Classified National Security Information"; E.O. 13549, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities"; and E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"); Management Directive (MD) 12.1, "NRC Facility Security Program"; MD 12.3, "NRC Personnel Security Program"; MD 12.4, "NRC Telecommunications Systems Security Program"; MD 12.5, "NRC Cyber Security Program"; and applicable directives of other Federal agencies and organizations.

II. OBJECTIVE

Ensure that all NRC personnel responsible for controlling, handling, and marking classified information (National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD)) and activities involving this information adhere to the procedures in this MD.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Chairman

1. As delegated by the President in E.O. 13526, Section 1.3, has original Top Secret classification authority.
2. Delegates original classification authority at the Top Secret and Secret levels to NRC personnel in accordance with E.O. 13526, Section 1.3. This authority may not be redelegated.

B. Commission

1. Approves the waiver of requirements normally applicable in furnishing classified information to foreign governments.
2. Acts on appeals for denial of information requested under the mandatory review procedures of E.O. 13526 when the request involves information generated by the Chairman, the Commissioners, or Commission-level offices.
3. Reviews and approves classification guides that could affect NRC major policy decisions before these guides are published.
4. As delegated by the Chairman, has original Top Secret classification authority.

C. Executive Director for Operations (EDO)

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

2. Designates the Senior Agency Official charged with overseeing classified information sharing and safeguarding efforts for the agency pursuant to the Commission-approved policy and program for implementing E.O. 13587.

3. Designates collectively the Deputy Executive Director for Corporate Management; the Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs; and the Deputy Executive Director for Reactor and Preparedness Programs as the NRC's Designated Approving Authority (DAA) for major information technology (IT) investments, to include IT investments associated with systems or networks on which classified information resides.

D. Deputy Executive Director for Reactor and Preparedness Programs (DEDR)

1. Designated as the Senior Agency Official who directs and administers the agency's program under which information is classified, declassified, controlled, handled, and marked; and actively oversees the implementation of E.O. 13526 by NRC employees, NRC contractors, NRC consultants, NRC licensees, and licensee-related organizations.

2. Issues and maintains guidelines for systematic review for declassification of 25-year old NSI under NRC jurisdiction and 40-year old classified foreign government information in NRC custody for use by the Archivist of the United States and, upon approval, by any agency holding the information.

3. Approves the designation of NRC personnel authorized to declassify or downgrade NSI.

4. Establishes and maintains an ongoing classified information self-inspection program, which includes regular reviews of representative samples of the agency's original and derivative classification actions.

5. Acts on appeals for denial of information requested under the mandatory review procedures of E.O. 13526 when the request involves information generated by offices and regions reporting to the EDO.

6. Ensures that the performance contract or other system used to rate personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of—

   (a) Original classification authorities;

   (b) Security managers or security specialists; and

   (c) All other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

E. Deputy Executive Director for Corporate Management (DEDCM)

1. Designated as the Senior Agency Official who directs and administers the agency's implementation and compliance with the National Industrial Security Program in accordance with E.O. 12829.
2. Designated as the NRC Senior Agency Official in accordance with E.O. 12968, to direct and administer the NRC's Personnel Security Program, including active oversight and implementation of continuing security education and awareness programs, and ensure that the order is effectively carried out.
3. Ensures that the NRC Facility Security Program is operated in an efficient and effective manner consistent with existing policies and regulations, and in a manner that protects against identified threats.
4. Approves plans for the protection of classified information in an emergency.

F. Inspector General (IG)

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

G. Office of the General Counsel (OGC)

1. Reviews any concerns regarding the legal aspects of the NRC transfer of information to foreign governments or international organizations.
2. Advises and assists the staff in developing procedures to comply with the Freedom of Information Act (FOIA) (5 U.S.C. 552).
3. Advises and assists the staff in initially determining whether particular records are exempt from disclosure, in whole or in part, in accordance with the *Code of Federal Regulations* (CFR) Title 10 Section 9.17, "Agency Records Exempt from Public Disclosure."
4. Advises and assists staff who make determinations for a FOIA (5 U.S.C. 522f) or a Privacy Act (PA) (5 U.S.C. 552a) appeal of the denial of records.
5. Interprets regulations in 10 CFR Part 9, "Public Records," Subpart A, "Freedom of Information Act Regulations," and Subpart B, "Privacy Act Regulations," as authorized by 10 CFR Section 9.5.
6. Provides legal advice on other problems arising under the FOIA and the PA, as requested.
7. Coordinates NRC activities relating to lawsuits under the FOIA and the PA.

H. Director, Office of International Programs (OIP)

1. As delegated by the Commission, determines if furnishing classified information to international organizations will result in a net advantage to the national security interests of the United States, subsequent to Commission approval of the initial request to exchange classified information with a foreign entity.
2. Assists with developing classified information exchange agreements with foreign countries or international organizations.

I. Secretary of the Commission (SECY)

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

J. Director, Office of Nuclear Security and Incident Response (NSIR)

1. Provides overall NRC information security program guidance and direction.
2. Provides mandatory Web-based Defensive Counterintelligence and Insider Threat Awareness training and Information Security (INFOSEC) Awareness training in coordination with the Office of the Chief Human Capital Officer (OCHCO), Human Resources Training and Development (HRTD), to be completed annually by all NRC employees and all U.S. citizen contractors working at the NRC headquarters campus facilities, NRC regional offices, and NRC training facilities, to include personnel with remote access to the NRC Local Area Network (LAN).
3. Designated as the Senior Agency Official charged with overseeing classified information sharing and safeguarding efforts for the agency in accordance with the Commission-approved policy and program for implementing E.O. 13587.

K. Director, Division of Security Operations (DSO), NSIR

1. Plans, develops, establishes, and administers policies, standards, and procedures for the NRC classified information security program, and manages the security classification program.
2. Coordinates the security aspects of the disclosure of classified information to foreign governments and international organizations.
3. Delegates derivative classification authority to NRC personnel. This authority may not be re-delegated.
4. Renders foreign ownership, control, or influence (FOCI) determinations and grants facility security clearances for NRC licensees.

5. As delegated by the Chairman, has original Secret classification authority.
6. Approves classification guides, except those requiring Commission approval.
7. Appoints the RD management official to serve as the primary point of contact for coordination with the U.S. Department of Energy (DOE) Director of Classification, on RD and FRD classification and declassification issues in accordance with 10 CFR Part 1045, "Nuclear Classification and Declassification."

L. Director, Office of Nuclear Material Safety and Safeguards (NMSS)

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

M. Director, Office of Information Services (OIS)

1. Manages non-IT information security policies for marking, handling, and protecting sensitive unclassified non-safeguards information.
2. Ensures cyber security requirements are properly incorporated into the agency's IT operations.

N. Director, Computer Security Office (CSO)

1. Plans, directs, and oversees the implementation of the agencywide Cyber Security Program, to include the electronic processing of classified information.
2. Responds to cyber security incidents, to include proper and timely reporting to the United States Computer Emergency Readiness Team (US-CERT).
3. Keeps the NRC apprised of current cyber security threats, vulnerabilities, and mitigation measures.

O. Office Directors and Regional Administrators

1. Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this MD.
2. Advise DSO, NSIR, and the Division of Facilities and Security (DFS), ADM, of any existing or proposed classified activities in organizations under their jurisdiction. Report any significant change or termination of classified activities to DSO, NSIR, and DFS, ADM, for review of associated contracts, subcontracts, or similar actions.
3. Furnish security plans to DSO, NSIR, and DFS, ADM, as appropriate.
4. Advise DSO, NSIR, and DFS, ADM, of any information that indicates noncompliance with this MD or is otherwise pertinent to the proper protection of classified interests and information.

5. Support and implement the NRC security classification program.
6. Control, handle, and mark classified information under their jurisdiction in accordance with this MD.
7. Request exceptions to or deviations from this MD as required.

P. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)

1. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program, including the approval of NRC facilities and NRC contractor facilities for handling and storing classified and sensitive unclassified information.
2. Administers the visitor control program, which covers visits requiring access to classified information.
3. Administers the NRC Security Infraction Program and coordinates action, as appropriate, with other NRC and Federal organizations regarding incidents of possible disclosure of classified information and other violations of Federal law or statutes.
4. Authorizes NRC employees and contractors to hand-carry classified documents (Secret and below) within the continental United States.
5. Approves and issues courier letters and courier cards to hand-carry classified information (Secret and below) off the NRC headquarters White Flint campus or an NRC regional facility.
6. Investigates and determines the eligibility of individuals for NRC access authorization and/or employment clearance.
7. Renders FOCI determinations and grants facility security clearances for NRC contractors.

IV. APPLICABILITY

The policy and guidance in this MD 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.

V. DIRECTIVE HANDBOOK

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

VI. EXCEPTIONS OR DEVIATIONS

The Director, NSIR, may grant exceptions to or deviations from this MD, in writing, except in those areas in which the responsibility or authority is vested solely with the Chairman, the Commission, the EDO, the DEDR, or the DEDCM and cannot be delegated. Exceptions or deviations to matters specifically required by law, E.O., or directive must be referred to other management officials.

VII. REFERENCES

Bureau of International Security and Nonproliferation

Bureau of International Security and Nonproliferation, "Agreement Between The United States of America and The International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto)," November 18, 1977, available at http://www.state.gov/t/isn/5209.htm.

Code of Federal Regulations

10 CFR Part 9, "Public Records":

Subpart A, "Freedom of Information Act Regulations."

Subpart B, "Privacy Act Regulations."

10 CFR Section 9.17, "Agency Records Exempt from Public Disclosure."

10 CFR Section 9.5, "Interpretations."

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

32 CFR Part 2001, "Classified National Security Information; Final Rule," June 28, 2010.

Department of Defense

National Industrial Security Program Operating Manual (NISPOM), available at http://www.dss.mil/documents/odaa/nispom2006-5220.pdf.

Executive Orders

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

E.O. 12968, "Access to Classified Information," August 4, 1995.

E.O. 13526, "Classified National Security Information," and related directives of the Information Security Oversight Office, National Archives and Records Administration, December 29, 2009.

E.O. 13549, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities," August 18, 2010.

E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

Federal Register Notices

Federal Register (FR) Notice, "Executive Order 13526 – Classified National Security Information Memorandum of December 29, 2009 – Implementation of the Executive Order "Classified National Security Information" Order of December 29, 2009 – Original Classification Authority," Vol. 75, No. 2, January 5, 2010, available at http://www.archives.gov/isoo/pdf/cnsi-eo.pdf.

FR Notice, "NRC Requirements Regarding Mandatory Review for Declassification," Vol. 61, No. 215, November 5, 1996, available at http://www.gpo.gov/fdsys/pkg/FR-1996-11-05/html/96-28373.htm.

National Disclosure Policy

National Disclosure Policy (NDP) 1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988.

National Security Decision Directives and Memoranda

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

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

Nuclear Regulatory Commission

Commission Papers (SECY)

COMSECY-04-0006, "Proposed Staff Discussions of Classified Information with the British, February 26-27, 2004," dated February 13, 2004 (Agencywide Documents Access and Management System (ADAMS) Accession Number ML040440300).

COMSECY-04-0034, "Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated June 14, 2004 (ADAMS Accession Number ML041900056).

COMSECY-10-0006, "Proposed Exchange of Classified and Safeguards Information with the United Kingdom – September 2010," dated June 8, 2010 (ADAMS Accession Number ML102090092).

Computer Security Office Standard (CSO-STD) 2004, "Electronic Media and Device Handling Standard," dated January 1, 2013 (ADAMS Accession Number ML100210148).

Delegations of Authority, Memorandum from—

Annette L. Vietti-Cook, Secretary, to Janice Dunn Lee, Director, Office of International Programs, "Staff Requirements – COMSECY-04-0034 – Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated July 7, 2004 (ADAMS Accession Number ML041900056).

Chairman Allison M. Macfarlane to Commissioner Kristine L. Svinicki; Commissioner George E. Apostolakis; Commissioner William D. Magwood, IV; Commissioner William C. Ostendorff; and R. W. Borchardt, Executive Director for Operations, "Delegation of Authority," dated November 29, 2012 (ADAMS Accession Number ML112010376).

Chairman Allison M. Macfarlane to Hubert T. Bell, Inspector General; Catherine Haney, Director, Office of Nuclear Material Safety and Safeguards; Patricia K. Holahan, Director, Division of Security Operations, Office of Nuclear Security and Incident Response; Bernard W. Stapleton, Chief, Information Security Branch, Division of Security Operations, Office of Nuclear Security and Incident Response, "Delegation of Authority," dated November 29, 2012 (ADAMS Accession Number ML112010327).

Chairman Allison M. Macfarlane to Mark A. Satorius, Executive Director for Operations, "Delegation of Authority," dated October 7, 2013 (ADAMS Accession Number ML13268A282).

Chairman Allison M. Macfarlane to Michael R. Johnson, Deputy Executive Director for Reactor and Preparedness Programs, Office of the Executive Director for Operations, "Delegation of Authority," dated November 29, 2012 (ADAMS Accession Number ML112010707).

R. W. Borchardt, Executive Director for Operations to Darren B. Ash, Deputy Executive Director for Corporate Management, Office of the Executive Director for Operations; Michael F. Weber, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, Office of the Executive Director

for Operations; Michael R. Johnson, Deputy Executive Director for Reactor and Preparedness Programs, Office of the Executive Director for Operations, "Designated Approving Authority for Major Information Technology Investments," dated June 13, 2012 (ADAMS Accession Number ML12083A054).

Electronic Information Exchange Web site: http://www.internal.nrc.gov/TICS/pdr/eie.html.

Management Directive—

3.1, "Freedom of Information Act."

3.2, "Privacy Act."

3.53, "NRC Records and Document Management Program."

12.0, "Glossary."

12.1, "NRC Facility Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

12.5, "NRC Cyber Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

13.1, "Property Management."

NUREG-0910, Revision 4, "NRC Comprehensive Records Disposition Schedule" (March 2005).

SECY 78-84, "Transfer of Classified Non-Military Information to Foreign Governments by NRC," dated April 14, 1978 (ADAMS Accession Number ML12272A645).

U.S. NRC Sensitive Compartmented Information Facility (SCIF) Security Guide and Standard Operating Procedure (SOP) (available from the Central Top Secret Control Officer).

Yellow Announcement YA-05-0077, "Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI)," October 26, 2005 (ADAMS Accession Number ML051220278).

Public Law

Public Law 111-258, "Reducing Over-Classification Act," October 7, 2010.

United States Code

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

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

Federal Records Act (44 U.S.C. 29, 31, and 33).

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

National Security Act of 1947 (50 U.S.C. 44).

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

DH 12.2 NRC CLASSIFIED INFORMATION SECURITY PROGRAM DT-17-226

Volume 12	Security
Approved by:	Mark A. Satorius Executive Director for Operations
Date Approved:	June 25, 2014
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.
Issuing Office:	Office of Nuclear Security and Incident Response Division of Security Operations
Contact Name:	Krista Ziebell 301-415-7121 Robert Norman 301-415-2278

EXECUTIVE SUMMARY

Directive and Handbook 12.2 are revised to incorporate new requirements of—

- Executive Order 13526, "Classified National Security Information," dated December 29, 2009;
- COMSECY-04-0006, "Proposed Staff Discussions of Classified Information with the British, February 26-27, 2004," dated February 13, 2004;
- COMSECY-04-0034, "Additional Steps to Regularize Clearances for Classified Information Exchanges with NRC's Primary Partner Countries," dated June 14, 2004;
- COMSECY-10-0006, "Proposed Exchange of Classified and Safeguards Information with the United Kingdom – September 2010," dated June 8, 2010, and the associated Staff Requirements Memorandum; and
- Other NRC policy changes that are related to information security requirements.

In addition, this revision incorporates recommended changes resulting from the Office of the Inspector General Audit 13-A-21, "Audit of NRC's Implementation of Federal Classified Information Laws and Policies," dated September 12, 2013, regarding the training requirements for original and derivative classification authorities, and classified information self-inspections.

TABLE OF CONTENTS

I. PROTECTION AND CONTROL OF CLASSIFIED INFORMATION 3

A. Scope 3
B. Classification 3
C. Control of Secret and Confidential Documents 32
D. Classification Guides 42
E. Classified Information Self-Inspections 43
F. Foreign Ownership, Control, or Influence (FOCI) 44

II. SPECIAL HANDLING OF CLASSIFIED INFORMATION 46

A. Control of Top Secret Documents 46
B. Naval Nuclear Propulsion Information 53
C. National Security Council Information (NSCI) 54
D. Transfer of Classified Information to Foreign Governments and International Organizations 57
E. Classified Conferences 64
F. Hand-carrying Classified Material 65
G. Transporting Classified Material by Commercial Airlines 66

EXHIBITS

Exhibit 1 Required Markings for Classified Documents 69
Exhibit 2 Declassification Markings 70
Exhibit 3 Subject or Title Marking and Portion-Marking 71
Exhibit 4 Upgrading, Downgrading, and Transclassification Markings 72
Exhibit 5 Deleting Classified Information From Classified Documents 73
Exhibit 6 Required Markings for an Unclassified Transmittal Document 74
Exhibit 7 Required Markings for a Classified Transmittal Document 75
Exhibit 8 Required Markings for Envelopes or Wrappers 76
Exhibit 9 Foreign Equivalent Markings 77

I. PROTECTION AND CONTROL OF CLASSIFIED INFORMATION

A. Scope

The procedures for classifying, declassifying, controlling, handling, and marking information to ensure a uniform system for protecting classified information against unauthorized disclosure are discussed in this handbook. These procedures implement the provisions of the Atomic Energy Act (AEA) of 1954, as amended; the Energy Reorganization Act of 1974, as amended; Public Law 111-258, "Reducing Over-Classification Act"; Executive Orders (e.g., E.O. 12829, "National Industrial Security Program"; E.O. 12968, "Access to Classified Information"; E.O. 13526, "Classified National Security Information"; E.O. 13549, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities"; and E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"); and other directives (e.g., directives of the Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA)).

B. Classification

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 people. Classification enables access to restricted information to properly cleared and authorized people who require access to perform official duties (see Management Directive (MD) 12.0, "Glossary," for the definition of terms utilized in this handbook).

1. Responsibility to Protect Classified Information

   (a) Reporting Unprotected Classified Information

   All personnel are responsible for protecting classified information in their custody and control. Any U.S. Nuclear Regulatory Commission employee or NRC consultant or contractor who finds classified information unprotected should take control of it and immediately contact the Division of Facilities and Security (DFS), Office of Administration (ADM), for guidance.

   (b) Classification Determination

   (i) A classification determination regarding NRC information, regardless of media, must be made solely by an NRC authorized classifier who has been delegated that authority and trained to exercise the authority. An authorized classifier is delegated either original or derivative classification authority.

(ii) An authorized classifier with original classification authority may classify information, on the basis of his or her knowledge, authority, and expertise, and if it is owned by, produced by or for, or is under the control of the U.S. Government and meets the requirements outlined in E.O. 13526, Section 1.4(a)-(h).

(iii) An authorized classifier with derivative classification authority may only classify information on the basis of classification determinations made by an original classification authority, a source document, or other classification guidance (e.g., a classification guide, a bulletin, or a notice). The AEA constitutes the authority for classification of Restricted Data (RD) and Formerly Restricted Data (FRD). Because the AEA classifies this information at its inception, all these classification determinations are derivative.

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

(c) Delegation of Classification Authority

(i) A *Federal Register* notice of January 5, 2010 (Vol. 75, No. 2) (available at http://www.archives.gov/isoo/pdf/cnsi-eo.pdf), designates the Chairman of the NRC as a Top Secret original classification authority under E.O. 13526, Section 1.3.

(ii) As authorized under E.O. 13526, Section 1.3, the Chairman has delegated Top Secret original classification authority to the four Commissioners, the Executive Director for Operations (EDO), and the Deputy Executive Director for Reactor and Preparedness Programs (DEDR).

(iii) As authorized under E.O. 13526, Section 1.3, the Chairman has delegated Secret original classification authority to the Inspector General (IG); the Director, Office of Nuclear Material Safety and Safeguards (NMSS); the Director, Division of Security Operations (DSO), Office of Nuclear Security and Incident Response (NSIR); and the Chief, Information Security Branch (ISB), DSO, NSIR.

(iv) Original classification authority cannot be delegated to NRC contractors.

(v) The responsibility for delegating derivative classification authority to NRC employees, NRC contractors, and other personnel has been assigned by the DEDR to the Director, DSO, NSIR.

(vi) The appropriate office director or regional administrator submits all requests for classification authority or changes to existing classification authority

(original or derivative), in writing, to the Director, DSO, NSIR. These requests must include—

- The names and positions of the individuals for whom authority is sought;
- Level of classification authority requested; and
- 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.

(vii) Upon receipt of the written request for classification authority, the Director, DSO, NSIR, will evaluate the request and take the necessary action to—

- Approve or disapprove a request for derivative classification authority;
- Refer to the Chairman to approve or disapprove a request for original classification authority; or
- Refer to the DEDR to approve or disapprove a request for declassification authority.

(viii) All NRC personnel who have been or will be granted an account to access any system or network (to include a stand-alone system or network) on which classified information resides must be an NRC authorized classifier.

(d) Authorized Classifier Training

(i) All authorized classifiers must be trained before they exercise their authority. ISB, DSO, NSIR, conducts classifier training when an individual is delegated classification authority.

(ii) ISB, DSO, NSIR, provides training materials to original classifiers, derivative classifiers, and declassifiers at headquarters and in the regional offices.

(iii) All original classification authorities must receive refresher training in proper classification (including avoiding over-classification) and declassification, as provided in E.O. 13526, and associated implementing directives at least once a calendar year. Training must include instruction on the proper safeguarding of classified information and the sanctions outlined in E.O. 13526, Section 5.5, that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive refresher training at least once a calendar year, as required by E.O. 13526, will have their classification authority suspended until the retraining is successfully completed.

(iv) All derivative classification authorities must receive refresher training in the proper application of the derivative classification principles of E.O. 13526,

with an emphasis on avoiding over-classification at least once every 2 years. Derivative classification authorities who do not receive the refresher training at least once every 2 years will have their classification authority suspended until the retraining is successfully completed.

(v) In accordance with E.O. 13526, Sections 1.3(d) and 2.1(d), original classification authority refresher training and derivative classification authority refresher training, respectively, can be waived by the Chairman or the DEDR if an individual is unable to receive the requisite training due to unavoidable circumstances. Whenever a waiver is granted, the individual must take the training as soon as possible.

(e) Responsibilities of Authorized Classifiers

(i) Each person possessing original or derivative classification authority is accountable for his or her classification actions and must apply the classification principles of E.O. 13526. Unnecessary classification, over-classification, and under-classification must be avoided.

(ii) An authorized classifier may make a classification determination only up to the level for which he or she has been delegated authority.

(iii) It is the responsibility of the authorized classifier to—

- Decide whether information requires classification;
- Determine the level and category of classification to be applied to the information; and
- Verify, if practical, that the classification guidance and the classification level are current before assigning a derivative classification.

(iv) An 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—

- Classification guides or other guidance approved for use (see Section I.D of this handbook);
- Previously declassified information; or
- Documents already determined to be unclassified.

(v) When an authorized classifier is in doubt about whether information is classifiable, the interpretation of a classification guide topic, which topic applies, or the proper level of classification, the matter should be promptly referred to the next higher classification authority or to DSO, NSIR, for a

determination (e.g., for derivative classification authorities, the next higher classification authority is an original classification authority). When there is reasonable doubt about the need to classify information or the appropriate classification level, the following actions must be taken—

- 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 an authorized classifier determines that the information should be classified, the information must be marked and protected accordingly (see MD 12.1, "NRC Facility Security Program," for the physical protection requirements for classified information).
- 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 (e.g., RD) that may be assigned to it, pending a determination about its classification level and the applicable category. When the classification level and category have been determined, the information must be marked and protected accordingly (see MD 12.1 for the physical protection requirements for classified information).

(vi) If an authorized classifier has significant doubt about the need to classify information, it will not be classified.

(vii) In all cases, a determination regarding classification must be made within 30 days in accordance with E.O. 13526.

(viii) Authorized classifiers also are responsible for ensuring that information they determine is classified is marked and protected accordingly (see MD 12.1 for the physical protection requirements for classified information).

(f) Responsibilities of an Originator

(i) If the originator of information is not an authorized classifier but believes that the information may require classification, he or she will 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 will handle it in accordance with MD 12.6, "NRC Sensitive Unclassified Information Security Program," and NRC Yellow Announcement YA-05-0077, "Policy Revision: NRC Policy and Procedures for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI)," October 26, 2005 (ADAMS Accession No. ML051220278).

(ii) If the originator of classified information is an authorized classifier, he or she will classify the information in accordance with the responsibilities identified in this handbook.

(iii) If the originator of information is routing information that may require classification for concurrence, then an authorized classifier will review and determine the classification of the information and requisite markings in accordance with Sections I.B.1–3 of this handbook in advance of routing the information for concurrence. Additionally, once the document has completed the concurrence route, an authorized classifier will review and reaffirm the prior classification determination and requisite markings in accordance with Sections I.B.1–3 of this handbook, to ensure that no edits to the content of the information during the concurrence route changed the classification and marking of the information.

(g) "No Comment Policy" for Classified Information

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

(h) Classification Challenges

(i) Authorized holders, including authorized holders outside the classifying agency, who are in authorized possession of classified National Security Information (NSI) and who in good faith believe that the classification level of the information is too high for its content (over-classification) or too low for its content (under-classification) are encouraged to challenge the classification status of that information.

- A person who wishes to challenge classification status must refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier will review the document and render a written classification decision to the holder of the information.

- In the event of a question regarding the classification review, the holder of the information or the authorized classifier will consult ISB, DSO, NSIR, for assistance.
- A person who challenges a classification decision has the right to appeal the decision to the Interagency Security Classification Appeals Panel (ISCAP). The ISCAP was created by the President in E.O. 13526, Section 5.3, to decide an appeal by an authorized person who has filed a classification challenge in accordance with Section 1.8 of E.O. 13526. ISB, DSO, NSIR, should be contacted in the event of an appeal.
- The NRC will provide an initial written response to a classification challenge within 60 days. If the NRC is unable to respond within 60 days, the NRC must acknowledge the classification challenge in writing and provide a date by which it will respond. If the NRC does not respond within 120 days, the challenger has the right to forward the challenge to the ISCAP for a decision.
- A person seeking to challenge the classification of information will not be subject to retribution.

(ii) Authorized holders, including authorized holders outside the classifying agency, who are in authorized possession of an RD or FRD document and who in good faith believe that the classification level of the information is improper are encouraged to challenge the classification with the RD classifier who classified the document as stated in Title 10 *Code of Federal Regulations* (CFR) Part 1045.39, "Challenging Classification and Declassification Determinations." In the event of a question regarding the classification review, the holder of the information or the RD classifier will consult with the NRC's RD management official for assistance.

(i) Limitations on Classification

(i) In accordance with Section 1.7, "Classification Prohibitions and Limitations," of E.O. 13526, information must not be classified to—

- Conceal a violation of the law, inefficiency, or an administrative error;
- Prevent embarrassment to a person, an organization, or an agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of national security.

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

(iii) Information may not be reclassified after declassification and release to the public under proper authority unless it meets one of the stated criteria in E.O. 13526, Section 1.7(c).

2. Classification of Protected Information

(a) Classification Process

Classification is the process of identifying information that needs protection in the interest of the national defense and foreign relations. This information must be designated as “National Security Information,” “Restricted Data,” or “Formerly Restricted Data.” Classification also involves determining the level and duration of classification and ensuring that information is properly marked. Among other considerations, a determination of whether or not information is classified must be made on the basis of the information that may be revealed by study, analysis, and/or observation, or use and/or by association with other information, including that which is known to be in the public domain. A classification determination 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 has been treated as unclassified in the general subject area.

(b) Types of Information that may be Classified in Each Category

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

(i) National Security Information (NSI)

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

- Military plans, weapons systems, or operations;
- Foreign government information;
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- Foreign relations or foreign activities of the U.S., including confidential sources;
- Scientific, technological, or economic matters relating to the national security;
- U.S. Government programs for safeguarding nuclear materials or facilities;

- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- The development, production, or use of weapons of mass destruction.

(ii) Certain information that would otherwise be unclassified may require classification (or classification to a higher level, i.e., Secret) when combined or associated with other classified or unclassified information. Classification on this basis must be supported by a written explanation that must be maintained with the file or record copy of the information. This practice is known as classification by compilation. NSI classified in accordance with this handbook must not be automatically declassified as a result of any unofficial publication or inadvertent or unauthorized disclosure of identical or similar information.

(iii) Restricted Data (RD) and Formerly Restricted Data (FRD)

The AEA is the basis for the determination that all RD and FRD are classified. Original classification authority and declassification authority for RD lie with the U.S. Department of Energy (DOE) under the AEA. Chapter 2 of the AEA defines RD and Section 142 establishes the basis for the concept of FRD. All RD and FRD classification actions are derived from the AEA. Current classification guidance conveys the types of information that must be designated as RD and FRD and the classification level that must be assigned to the information. This classification guidance may be obtained from ISB, DSO, NSIR.

(c) Levels of Classification

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

(ii) A Special Access Program is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. The number of people who have access to this information is reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(iii) Sensitivity of the Information

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

disclosure of Confidential information is presumed to cause damage to the national security, Secret disclosure presumes serious damage, and Top Secret disclosure presumes exceptionally grave damage.

(iv) Classification Authority

Classification authority for NSI is the authorized original classifier, a classification guide, or a source document, as prescribed by E.O. 13526. The classification authority for RD or FRD is the AEA, as conveyed by classification guides.

(v) Duration of Classification

- The duration of classification is the length of time the information must remain classified. For original classifications, NSI must be classified in accordance with E.O. 13526. At the time of original classification, the original classifier shall attempt to identify a specific date or event for declassification that is less than 10 years from the date of the original classification. If the original classifier cannot determine a date or event for declassification, the information shall be marked for declassification 10 years from the date of original classification unless the original classification authority determines the sensitivity of the information requires that it shall be marked for declassification 25 years from the date of the original decision.
- Records of permanent historical value should be declassified in accordance with E.O. 13526, Section 3.3 (see Section I.B.5 of this handbook for declassification of NSI).

(vi) Declassification Exemptions

NSI may be exempted from declassification within 10 years if the information could reasonably be expected to cause damage to the national security and it qualifies for exemption in accordance with E.O. 13526, Section 3.3(b). Normally, exemption from declassification may not exceed 25 years (see Section I.B.5 of this handbook for declassification of NSI).

(vii) Classification Extensions

If NSI cannot be declassified on the specific date or event for declassification set at the time of classification, an original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information in E.O. 13526, are followed. An original classification authority may extend the duration of classification for information contained in nonpermanent records beyond 25 years in accordance with the standards and procedures for

classifying information. Except for information that identifies a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, all other information shall identify a specific date or event for declassification, not to exceed December 31 of the year that is 50 years from the date of origin of the records (see Section I.B.5 of this handbook for declassification of NSI).

(viii) Information Classified Under Previous Executive Orders

No information can remain classified indefinitely. NSI marked “Originating Agency's Determination Required” (OADR) in previous E.O.s may be declassified if the information is declassifiable according to E.O. 13526. The information may be re-marked to establish the duration of classification consistent with the requirements of E.O. 13526 or if the information is of permanent historical value, it may remain classified for 25 years from the date of original classification. After that time, it will be automatically declassified in accordance with E.O. 13526, Section 3.3 (see Section I.B.5 of this handbook for declassification of NSI).

(ix) Restricted Data and Formerly Restricted Data Exemption

RD and FRD are exempt from automatic declassification. AEA Sections 141 and 142 set forth the policy regarding review and declassification of RD and transfer of information from the RD category to the FRD status (see Section I.B.5 of this handbook for declassification of RD and FRD).

3. Marking Classified Documents

(a) Portion-Marking

(i) Each section, part, paragraph, or similar portion (e.g., subjects, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks) of a classified document must be marked to show the highest level of classified material and most restrictive category, or that the portion is unclassified (see Exhibit 3 of this handbook). Portions of a document must be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. Each portion of a document containing NSI must be marked. A document containing RD or FRD is not required to be portion-marked.

(ii) To mark portions of the text in a classified document, one of the following appropriate classification abbreviations is placed parenthetically immediately preceding the portion to which it applies (e.g., titles, graphics, bullet statements, and subjects).

- (TS) for Top Secret

- (S) for Secret
- (C) for Confidential
- (U) for Unclassified

(iii) To the extent practicable, do not commingle RD and/or FRD and NSI in the same document. If a document contains a combination of categories of classified information, the highest level of classified information must be coupled with the most restrictive category and placed parenthetically immediately before the text it governs.

- (RD) for Restricted Data
- (FRD) for Formerly Restricted Data
- (NSI) for National Security Information
- For example: (CRD), (SRD), or (TSNSI)

(iv) If a commingled document is not portion-marked, then it shall not be used as a source for a derivatively classified document.

(v) 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.

(b) Overall Marking

(i) When preparing a classified document, 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).

(ii) The highest overall classification level of the entire document must be placed at the top and bottom of each interior page. However, for RD, a classifier must ensure that a document containing RD and FRD is clearly marked at the top and bottom of each interior page with the overall classification level and category.

(iii) In all cases, the markings displayed in Exhibit 1 of this handbook must be placed on the face of all classified documents, the front cover, the title page, or the first page of each classified document.

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

(c) Classification Markings for National Security Information (NSI)

(i) Information classified in accordance with E.O. 13526 must show the name and the position title of the original classifier or personal identifier; the agency and office of origin, if not otherwise evident; the specific reason for classification, as identified in E.O.13526, Section 1.4; and the declassification instructions indicating the decision for the duration of the classification.

(ii) An example of an original classification marking is as follows:

- Classified By: Insert name of original classifier, position title, and authorized classifier number
- Reason: Insert reason from E.O. 13526, Section 1.4
- Declassify On: Insert date or event for declassification

(iii) An example of a derivative classification marking follows:

- Derived From: Insert name of classification guide or source document and date
- Reason: Insert reason from E.O. 13526, Section 1.4
- Declassify On: Insert date or event for declassification
- Classifier: Insert name of derivative classifier, position title, and authorized classifier number

(iv) For original classification decisions, if an original classification authority cannot determine an earlier specific date or event for declassification, NSI must be marked for declassification 10 years from the date of the original classification. If it is determined that NSI must remain classified longer than 10 years, the original classification authority must cite a date that is 25 years from the date of original classification in accordance with E.O. 13526, Section 1.5.

(v) For derivative classification decisions, the derivative classification authority shall carry forward the instructions on the “Declassify On” line from the source documents to the derivative document, or the duration instruction from the classification guide. If the source document is missing the declassification instructions, then a date of 25 years from the date of the source document (if available) or the current date (if the source document date is not available) will be carried forward by the derivative classification authority.

(vi) Except in extraordinary circumstances, or as approved by the Director, ISOO, the marking of classified information must not deviate from the requirements identified in Section I.B.3 of this handbook. Requests for waivers should be

addressed to the Director, DSO, NSIR, who will evaluate the request and either forward the request to the Director, ISOO, or return the request with comments as to why the request was not forwarded to ISOO.

(d) Reclassification of Information

If it is determined that NSI must be reclassified after being declassified and released to the public, the action is requested in writing by the NRC Chairman as identified in E.O. 13526, Section 1.7. Upon reclassification, the new classification must appear on the first page of the document. The overall classification should include the following text, on the front page, and in a manner that is immediately apparent:

This document has been reclassified in accordance with E.O.13526, Section 1.7, by authority of the Chairman of the NRC.

(e) Classification Markings for RD and FRD

(i) RD and FRD will not have the same classification markings as NSI. RD and FRD are never subject to automatic declassification.

(ii) A document classified as RD will have the following notice stamped in the lower left of the first page of the document:

RESTRICTED DATA

This Document Contains Restricted Data as Defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal sanctions.

(iii) A document classified as FRD but that does not contain RD will have the following notice stamped in the lower left of the first page of the document:

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to Administrative and Criminal sanctions. Handle as Restricted Data in Foreign Dissemination, Section 144b Atomic Energy Act of 1954.

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

Classified By: Insert name of classification guide or source document and date

Derivative Classifier: Insert name of derivative classifier, position title, and authorized classifier number

(f) Mixed Levels and Categories

(i) When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized access to if the document was only marked at the highest overall classification level and category. (For example, a document that contains Confidential RD and Secret NSI would be required to be marked as Secret RD, the highest level and most restrictive category. None of the information in the document is Secret RD). However, this may not be interpreted to authorize any individual to gain access to information that exceeds their security clearance, formal access approvals, and need to know.

(ii) If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking.

This document contains:

Restricted Data at the (e.g., Confidential) level

Formerly Restricted Data at the (e.g., Secret) level

National Security Information at the (e.g., Secret) level

Classifier: Insert name of authorized classifier, position title, and authorized classifier number

(g) Authorized Sources for Classification

(i) Authorized sources for classification of NSI are an original classification authority, a source document, or other classification guidance (e.g., a classification guide, a bulletin, or a notice).

(ii) Authorized sources for classification of RD and FRD are a source document or other classification guidance (e.g., a classification guide, a bulletin, or a notice). DOE has original classification authority for RD in accordance with the AEA. NRC may not make original classification decisions for RD.

(iii) If a document is classified on the basis of more than one source document or classification guide, the phrase "Multiple Sources" must be cited as the classification authority on the "Derived From" line. The derivative classifier must include a listing of the source materials on, or attached to, each derivatively classified document. The date of declassification marking on

multiple-source documents will reflect the source that provides the longest period of classification.

(h) Declassification Markings

(i) NSI may be declassified by—

- The originator who authorized the original classification, if that official is still serving in the same position and has original classification authority;
- The originator's current successor in function, if that individual has original classification authority;
- A supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or
- An individual delegated declassification authority in writing by the DEDR.

(ii) RD may be declassified by people appointed by DOE.

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

- This document has been declassified under the provisions of E.O. 13526, dated December 29, 2009.
- Declassified By: Insert name of declassifier, position title, and authorized classifier number
- Date of Declassification: Insert date of declassification

4. Change of Classification and Marking

(a) Upgrading

(i) A notice that a document containing NSI was mistakenly issued as unclassified or was mistakenly declassified, must be classified and marked at an appropriate level, but not lower than Confidential. A notice that a document containing RD was issued as unclassified or was mistakenly declassified must be classified and marked at least "CRD" (Confidential Restricted Data). If the notice contains information requiring a higher classification or a more restrictive category, the notice must be marked accordingly (see Exhibit 1 of this handbook for placement of markings).

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

- Title, subject, or a brief description of the document;
- Document number, if any;

- Author of the document;
- Date of the document;
- Person authorizing the classification or upgrading;
- Portions of the document to be classified or upgraded, if appropriate; and
- All markings, including portion-markings, to be placed on the document.

(iii) The notice will be distributed to all regional administrators and office directors; the Secretary of the Commission (SECY); the Office of Information Services (OIS); the Chief, Facilities Security Branch (FSB), DFS, ADM; and all known holders of the document, as determined by DSO, NSIR.

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

(v) After all copies of the document have been properly accounted for and re-marked or destroyed, the notice may be declassified, unless the content of the notice is classified (see Section I.B.5 of this handbook for declassification).

(vi) 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.

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

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

- Classification Changed To: Insert new classification level
- By Authority Of: Insert name of person authorizing change, position title, and authorized classifier number
- By: Insert signature of person making change
- Date: Insert date of change

(b) Downgrading

(i) NSI may be downgraded by-

- The originator who authorized the original classification, if that official is still serving in the same position and has original classification authority;
- The originator's current successor in function, if that individual has original classification authority;
- A supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or
- An individual delegated declassification authority in writing by the DEDR.

(ii) RD may be downgraded by people appointed by DOE.

(iii) DSO, NSIR, should be consulted for downgrading instructions. RD and FRD may only be downgraded in accordance with approved DOE classification guidance (e.g., classification guides or bulletins).

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

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

- Title, subject, or a brief description of the document;
- Document number, if any;
- Originator of the document;
- Date of the document;
- Person authorizing the downgrading and the position title of the original individual, or personal identifier;
- New classification level that will be assigned to the document;
- Effective date of the change; and
- If appropriate, the portions of the document to be downgraded.

(vi) 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.

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

(viii) 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.

- Classification Changed To: Insert new classification level
- By Authority Of: Insert name of person authorizing change, position title, and authorized classifier number
- By: Insert signature of person making change
- Date: Insert date of change

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

(x) 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 will refer the matter to the Director, DSO, NSIR.

(c) Transclassification

(i) "Transclassification" means information that has been removed from the RD category in order to carry out provisions of the National Security Act of 1947,

as amended, and safeguarded under applicable E.O.s as NSI (see MD 12.1 for the physical protection requirements for classified information).

(ii) In accordance with Section 142(d) of the AEA, FRD is classified information related primarily to the military utilization of atomic weapons that has been removed from the RD category after the DOE and U.S. Department of Defense (DoD) have jointly determined that the information can be adequately protected in a manner similar to NSI.

(iii) In accordance with Section 142(e) of the AEA, Transclassified Foreign Nuclear Information (TFNI) is classified information concerning foreign nuclear programs that has been removed from the RD category for intelligence purposes after the DOE and the Director of National Intelligence (DNI) have jointly determined that the information can be adequately protected in a manner similar to NSI.

(iv) All transclassification actions must occur in accordance with AEA Sections 142(d) and (e) and must take place only upon written notification of this change by the Director, DSO, NSIR. Contact DSO, NSIR, when it is necessary to transclassify information.

(v) Upon receipt of a transclassification notice, the person responsible for the transclassification will cross out the existing RD marking and insert the FRD or TFNI marking below or beside the marked-out classification, as applicable (see Exhibit 4 of this handbook), along with any other additional identifiers that are prescribed by DOE. Additionally, the following statement must be placed on the face of the document, the cover, the title page, or the first page of text.

- Classification Changed To: Insert new classification level
- By Authority Of: Insert name of person authorizing change, position title, and authorized classifier number
- By: Insert signature of person making change
- Date: Insert date of change

5. Declassification of Classified Information

(a) Authorities

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

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

(b) Automatic Declassification

(i) Subject to E.O. 13526, Sections 3.3(b)–(d) and (g)–(j), all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value in accordance with United States Code (U.S.C.) Title 44, "Public Printing and Documents," will be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in E.O. 13526, Sections 3.3(b)–(d) and (g)–(j). If the date of origin of an individual record cannot be readily determined, the date of original classification will be used instead.

(ii) In accordance with E.O. 13526, Section 3.3(b), information may be exempted from automatic declassification at 25 years if its release would clearly and demonstrably be expected to—

- Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;
- Reveal information that would assist in the development, production, or use of weapons of mass destruction;
- Reveal information that would impair U.S. cryptologic systems or activities;
- Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;
- Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;
- Reveal information, including foreign government information, that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S.;

- Reveal information that would impair the current ability of U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;
- Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or
- Violate a statute, a treaty, or an international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(iii) All records exempted from automatic declassification under E.O. 13526, Sections 3.3(b) and (c) shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin.

(iv) In accordance with E.O. 13526, Section 3.3(h), information may be exempted from automatic declassification at 50 years if its release would clearly and demonstrably be expected to reveal the following—

- The identity of a confidential human source or a human intelligence source; or
- Key design concepts of weapons of mass destruction.

(v) All records exempted from automatic declassification under E.O. 13526, Section 3.3(h), shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless, within 5 years of that date, the Chairman, in coordination with ISB, DSO, NSIR, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the ISCAP.

(vi) If a review or assessment has determined the information within that file series almost invariably falls within one or more of the exemption categories listed in item (ii) or (iv) of this section, at least 2 years before information is automatically declassified under E.O. 13526, Section 3.3, the holder of the information or the reviewer will consult ISB, DSO, NSIR, for assistance in submitting a request for exemption from automatic declassification at 25 or 50 years, respectively, to the ISCAP in accordance with E.O. 13526, Section 3.3(j).

(c) Declassification Reviews

(i) Any declassification review of documents that may contain classified information from other agencies or that may be of direct interest to other agencies will be coordinated with the affected agencies by the Director, DSO, NSIR.

(ii) Standard Declassification Reviews

- Standard declassification reviews result from a request within the NRC, from NRC contractors or other organizations associated with an NRC program, or from other Government agencies to review documents for declassification. Information is subject to review for declassification under several circumstances: (1) a request (e.g., under the Freedom of Information Act (FOIA)), (2) a mandatory review, or (3) a systematic review. In these cases, a request for declassification of NSI must be forwarded to the authorized classifier responsible for the original classification, his or her successor, a supervisor of either with the required declassification authority, or the Director, DSO, NSIR. RD and FRD will be declassified in accordance with the provisions of Section I.B.5(a)(ii) of this handbook.
- FOIA or Privacy Act (PA) declassification reviews and other actions involving review of classified information in accordance with the FOIA or the PA must be conducted in accordance with the provisions of this section and MD 3.1, “Freedom of Information Act,” and MD 3.2, “Privacy Act.” The handling and retention of classification information must also comply with the “Federal Records Act”; MD 3.53, “NRC Records and Document Management Program”; and NUREG-0910, “NRC’s Comprehensive Records Disposition Schedule."
- The Director, DSO, NSIR, will attempt to resolve any disagreements on the releasability of information contained in classified documents that are requested under the FOIA or the PA.
- If NRC receives a FOIA or a 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. When 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.

(iii) Mandatory Declassification Reviews

NRC information classified under E.O. 13526 or earlier E.O.s (e.g. E.O. 12958, as amended) is subject to a review for declassification under provisions of E.O. 13526, Section 3.5. All such declassification reviews will be conducted in accordance with the "NRC Mandatory Review for Declassification Procedures," published in the *Federal Register* (61 FR 56974) on November 5, 1996, and available from DSO, NSIR, upon request.

(iv) Systematic Review for Declassification

All NRC classified information is subject to systematic review for declassification under the provisions of E.O. 13526, Section 3.4. All such declassification reviews will be conducted in accordance with the NRC systematic review guidelines, which are available from DSO, NSIR, upon request. As stated in Section 5.2(b) of E.O. 13526, the Director, ISOO, will review and approve implementing regulations and agency guides for systematic declassification review before issuance by the NRC.

(v) Notice of Declassification

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 must notify the Director, DSO, NSIR, who in turn must notify custodians of all copies.
- Secret or Confidential Documents. The individual authorizing the declassification of a Secret or Confidential document will 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, DSO, NSIR.
- Contents of the Notice. Declassification notices must identify the document as fully as possible, stating the title, the subject, or a brief description of the document; the document number, if any; the originator of the document; the date of the document; the person authorizing the declassification; and the effective date of the declassification. These notices will normally be unclassified unless some unusual circumstances require the inclusion of classified information.
- Forwarding of the Notice. If the recipient of a declassification notice has forwarded the document to another custodian, the declassification notice also must be forwarded to the other custodian. However, for documents declassified under the automatic declassification provision of E.O. 13526, Section 3.5, a notification is not necessary because these documents are

official agency records that are publically available in the Agencywide Documents Access and Management System (ADAMS) after declassification.

6. Deletion of Classified Information From Documents

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

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

   (c) An authorized classifier from the office that originated the document will identify the classified information to be redacted from the document. DSO, NSIR, is available for consultation to ensure that all classified information is identified for redaction.

   (d) After identifying the classified information, the responsible person must ensure that the classified information is redacted from the document and strike through the category and classification authority markings that appear on the front cover, title page or first page, and the classification at the top and bottom of each page. If the document is bound, only the classification on the front cover, the title page, the first and the last page of text, and the outside back cover need to be struck through. Note: all classified information must be redacted from each page.

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

      The classified information has been removed from this document.

      This copy of the document is UNCLASSIFIED.

      By Authority of: Insert name of person authorizing change, position title, and authorized classifier number

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

7. Markings for Specific Types of Classified Information

(a) Transmittal Documents

(i) Unclassified Transmittal Documents

- The classification marking on the first page of an unclassified transmittal document must be equivalent to the highest level of classification being transmitted. Other pages of the transmittal document must have the same classification marking.
- The lower right side of the first page of the transmittal must be marked to indicate the level of information contained in the transmittal letter when standing alone; for example, when separated from the classified enclosure, this transmittal is unclassified.
- If the information is RD, the lower left side of the first page of the transmittal document must be marked to identify it as transmitting RD (see Exhibit 6 of this handbook).

(ii) Classified Transmittal Documents

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

- 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.
- 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.
- If the category of classified information identified for the transmittal document is NSI and the other document(s) being transmitted is (are) RD/FRD, the lower left side of the transmittal must also be marked “RD/FRD” to reflect the most restrictive category of classified information being transmitted.
- 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 I.B.4 - 5 of this handbook, respectively, must be followed.

(iii) Compilations

A compilation composed of existing information from several sources must be treated as a new document and classified and marked in accordance with Sections I.B.2–3 of this handbook. 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.

(iv) Files or Folders Containing Classified Documents

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 in the file or folder or, if warranted by compilation, a higher classification level.

(b) Drafts and Working Copies

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

(ii) Other markings (e.g., classification authority, duration, portion-marking, and documentation) are not required unless the document will be distributed outside the preparing office or maintained for file, record, reference, background, or historical purposes. Drafts and working copies retained for more than 180 days must be marked to include all classification and declassification information. In these instances, the document must be classified and entered into the automated Classification Management Actions (CMA) system in accordance with Section I.B.8 of this handbook.

(iii) Top Secret documents must be documented in accordance with Section II.A of this handbook, except that the series designator must be assigned as “Draft 1,” “Draft 2,” and so forth, or “Working Copy 1,” “Working Copy 2,” and so forth, instead of a letter of the alphabet.

(c) Reproduction and Dissemination Limitations

(i) 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:

> Reproduction or further dissemination requires approval of Insert title of authorizing official.

(ii) See MD 12.1 for procedures for reproducing Secret and Confidential documents. See Section II.A of this handbook for procedures for reproducing Top Secret documents.

(d) Foreign Government Information

(i) Information received from foreign governments must either retain its original classification designation or be assigned a U.S. classification level that will ensure a degree of protection at least equivalent to that required by the entity that furnished the information (see Exhibit 9 of this handbook for "Foreign Equivalent Markings"). In addition, the 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.

(ii) A document originated by the NRC that contains foreign government information must be marked in accordance with Section I.B.3 of this handbook and, if applicable, assigned a U.S. classification level that will ensure a degree of protection at least equal to that afforded equivalent U.S. information. The document also must be identified with the "FOREIGN GOVERNMENT INFORMATION" marking. Any paragraph that contains foreign government information must be identified by placing the designator "FGI" in parentheses before or after the text it governs.

(iii) 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 I.B.3 of this handbook, as if it were wholly of U.S. origin.

(e) Electronic Media

(i) Electronic media that contains classified information must be marked in accordance with MD 12.5, "NRC Cyber Security Program," and Computer Security Office Standard 2004 (CSO-STD-2004), "Electronic Media and Device Handling Standard."

(ii) NRC personnel who need to mark electronic media that contains classified information should use the pre-printed labels available for that purpose (available in the NRC supply room). If the use of pre-printed labels impairs the

functionality of the electronic media, then a permanent marker should be used to prominently mark electronic media in accordance with MD 12.5 and CSO-STD-2004.

(f) Translations

Translations of U.S. classified information into a language other than English must be marked in accordance with this section. Translations also must be marked to show the United States as the country of origin and with the foreign language equivalent markings (see Exhibit 9 of this handbook for "Foreign Equivalent Markings").

8. Classification Management Actions (CMA) System

(a) The CMA system is an automated system that allows DSO, NSIR, to record information about each classification decision made by NRC authorized classifiers. The system is used to collect and record NRC Form 790, “Classification Record.” The NRC Form 790 is available in the NRC Forms Library on the NRC SharePoint site (available at http://portal.nrc.gov/nrcformsportal/default.aspx). The NRC Form 790 is completed manually by a licensee, certificate holder, NRC contractor, or NRC employee delegated classification authority. The authorized classifier submits the original NRC Form 790 to DSO, NSIR. DSO, NSIR, monitors all data index input and maintains the CMA system's records.

(b) The NRC Form 790 is required each time an authorized classifier makes a decision to classify, declassify, or downgrade a document. The information contained on the completed form includes specific information that identifies the document being classified, declassified, or downgraded, as well as specific information describing the status (e.g., original or derivative classification, the reason for the declassification review, or future action) of the classified document. This information enables the NRC to conduct assessments of classification, downgrading, or declassification decisions made by those officials specifically authorized to make such determinations and to prepare accurate feeder data into an annual report to the ISOO.

(c) DSO, NSIR, is responsible for preparing specific reports on classification actions that are taken on the basis of information provided by the CMA system and for submitting these reports to ISOO as required. The CMA system enables DSO, NSIR, to verify proper classification actions during self-inspections or audits in order to effectively administer the NRC Classified Information Security Program.

C. Control of Secret and Confidential Documents

1. Cover Sheets

   (a) A “SECRET” cover sheet, Standard Form 704, or a “CONFIDENTIAL” cover sheet, Standard Form 705 (available in the NRC supply room at headquarters and in each region), must be placed on the face of each copy of a document classified as Secret or Confidential upon preparation, or upon receipt from outside sources if no form is attached. Appropriate marking instructions and selected handling procedures can be found on the reverse side of the cover sheets.

   (b) The cover sheet must remain on the copy whether the copy is held by an NRC employee, NRC contractor, or subcontractor, or transmitted to other destinations. The cover sheet should be retained on a Secret or Confidential document in the file.

   (c) If removed, the cover sheet must be placed on a document when it is withdrawn from the file and must remain with the document until the document is returned to the security storage container or destroyed.

   (d) Upon destruction of the document, the cover sheet may be removed and, depending on its condition, reused.

2. Assurances Required Before Transmitting Classified Information

   (a) Before the transmission of classified information, regardless of the means (e.g., verbally, electronically, or manually), the holder of classified information must ensure that the recipient has a need-to-know, is authorized to receive the information, possesses the appropriate access authorization, and has approved storage facilities for protecting classified information. The holder of classified information may obtain assurance of this information from DFS, ADM, or the recipient's cognizant security office. The following types of questions should be considered when a holder of classified information is making a need-to-know determination:

      (i) What is the topic/subject of the information being transmitted?

      (ii) Who is requesting the information?

      (iii) What is the purpose and basis of the request?

      (iv) Was the request previously submitted or identified (i.e., through an inspection plan, interagency agreement, memorandum of understanding)?

      (v) What is the sensitivity of the requested information (i.e., NSI, RD, FRD, special access considerations)?

(vi) Is the NRC the originator of the requested information or was the information provided by an outside source (i.e., other government agency, foreign government, or licensee)?

(vii) Has the originator of the requested information received similar requests, presently or historically?

(viii) Is the requested information relevant to the requestor's official duties?

(ix) Is the requested information necessary for the performance of the requestor's official duties?

(b) In cases where the holder of classified information is not satisfied that the recipient possesses a demonstrable need-to-know or, in cases of non-routine access to classified information, the holder of classified information should consult ISB, DSO, NSIR, for assistance.

(c) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the Chairman or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access, in accordance with E.O. 13526, Section 4.2(b).

(d) Before delivering a hand-carried classified document to the addressee or the authorized recipient, the individual delivering the document will require positive identification of the addressee or the recipient. Authority for NRC employees or NRC contractors to hand-carry classified documents (Secret and below) within the continental U.S. must be granted by the Director, DFS, ADM, or a designated alternate identified in writing by the Director, DFS, ADM.

(e) The removal of a classified document from an approved facility to a private residence or other unapproved place for work purposes is prohibited. Also, leaving a classified document unattended in a motel or hotel during official travel is prohibited.

(f) A classified document, when not in the possession of an authorized individual, must be stored only in an approved facility (see MD 12.1 for storage of classified documents).

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

3. Means of Transmission of Secret Documents Inside the United States

(a) A person hand-carrying a Secret document shall keep the document continuously in his or her possession until the document is stored in an approved facility. A courier letter or a courier card approved and issued by the Director,

DFS, ADM, or a designated alternate identified in writing by the Director, DFS, ADM, is required when hand-carrying classified information off the NRC headquarters campus or an NRC regional facility (see Section II.F of this handbook for more details on hand-carrying classified information).

(b) A Secret document transmitted internally within facilities must be hand-delivered by a person authorized access to the information or transmitted by approved internal mail service.

(c) A Secret document transmitted externally to an outside facility must be delivered by—

(i) A method approved for the transmission of a Top Secret document in accordance with Section II.A.9 of this handbook;

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

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

(iv) A commercial delivery company approved by DFS, ADM, that provides nationwide, overnight service with computer tracking and reporting features. (The company does not need a security clearance.)

4. Means of Transmitting Secret Documents Outside the United States

(a) 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, ADM, and assurance that the information will not pass out of control of U.S. citizens or through a foreign postal system. This method may be used to transmit a Secret document to and from the U.S. Government or a contractor employee or a member of the Armed Forces in a foreign country.

(b) U.S. Department of State diplomatic pouch. A document may be transmitted to a U.S. Government employee, a contractor employee, or a member of the Armed Forces in a foreign country by use of the U.S. Department of State diplomatic pouch. This method must be approved by the Director, DFS, ADM, before it is used. The approval may be granted for an individual transmission or on a blanket basis.

(c) An authorized person hand-carrying a Secret document to and from foreign countries. The approval of the Director, DFS, ADM, must be obtained before hand-carrying a Secret document to or from a foreign country. Arrangements must be made to preclude the necessity for customs examination of the

document. An employee transporting a Secret document must use a vehicle or aircraft owned by the U.S. Government or its contractors, a ship of the U.S. Navy, a U.S. naval ship manned by the civil service, or a ship of U.S. registry. Hand-carrying a Secret document to and from foreign countries may be permitted only when other means set forth above are impractical and it is necessary to perform official duties.

5. Means of Transmitting a Confidential Document Inside and Outside the United States

   (a) A person hand-carrying a Confidential document must keep the document continuously in his or her possession until the document is stored in an approved facility or is turned over to a designated recipient. A courier letter or a courier card approved by the Director, DFS, ADM, is required when hand-carrying classified information off of the NRC headquarters campus or an NRC regional facility (see Section II.F of this handbook for more details on hand-carrying classified information).

   (b) A Confidential document transmitted internally within facilities must be hand-delivered by a person authorized access to the information or transmitted by an approved internal mail service.

   (c) A Confidential document transmitted externally to an outside facility must be delivered by—

      (i) A method approved for the transmission of a Secret document; or

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

6. Electronically Transmitting Classified Messages

   (a) A Classified message must be transmitted only by electronic means that are protected with National Security Agency- (NSA) approved encryption and that have been approved by DSO, NSIR, and CSO. Transmission of classified information in ADAMS or in the Electronic Information Exchange (http://www.internal.nrc.gov/TICS/pdr/eie.html) is prohibited.

   (b) Procedures applicable to handling classified messages within approved communications centers are set forth in MD 12.4, “NRC Telecommunications Systems Security Program,” and MD 12.5.

   (c) All paper copies of an electronically transmitted classified message must be marked in accordance with Sections I.B.2–3 of this handbook. Classification marking in the electronic environment must be completed in accordance with

32 CFR, “National Defense,” Part 2001, “Classified National Security Information,” Section 2001.23.

(d) Portion-marking must be used to identify the classified and unclassified portions of the message, to include the subject lines. Text must be portion-marked in accordance with Sections I.B.3(c)–(e) of this handbook.

(e) The overall classification marking for the message must be placed at the top and bottom of the body of each message. The overall classification for the message will reflect the classification of the header and the body of the message, to include the subject line, the signature block, attachments, and any other information conveyed in the body of the message. The classification markings must be placed after the signature block, but before the overall classification marking string at the end of the e-mail. Classification markings must be completed in accordance with Section I.B.3(a) of this handbook.

(f) When forwarding or replying to an e-mail, the markings shall reflect the overall classification and declassification instructions for the entire string of e-mails and attachments.

(g) Upon receipt of a classified message, the transmitting communications center person will—

(i) Review the message to determine that required security classification markings have been applied to the form and the message;

(ii) Encrypt, transmit, or otherwise dispatch the message in accordance with MD 12.4 and MD 12.5;

(iii) Return to the originating office all messages containing notations, if requested; and

(iv) Destroy all copies of a classified message in the center's possession 90 days after transmission unless a longer period is approved by the Director, DSO, NSIR.

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

(i) Decrypt and edit the message as prescribed by MD 12.4 and MD 12.5 and add the security markings in accordance with Sections I.B.2–3 of this handbook;

(ii) Ensure that the message is given to the addressee;

(iii) Destroy all copies of a classified message in the center's possession 90 days after receipt unless a longer period is approved by a regional administrator or the Director, DSO, NSIR; and

(iv) Maintain records of the destruction of all Top Secret messages, if applicable.

7. Documents Transmitted from Other Agencies

(a) A classified document originated by another agency and created prior to June 25, 2010 (effective date of E.O. 13526), must not be disseminated outside of the NRC without the consent of the originating agency. Any other classified document that has been originated by another agency and created on or after June 25, 2010, may be disseminated outside of the NRC or an NRC contractor office, when needed, unless the document in question clearly states that permission must be obtained prior to further dissemination.

(b) If permission is granted, the transmission must be handled in accordance with Sections I.C.3–5 of this handbook.

(c) A copy of the documentation of the permission to transmit a classified document from another agency must be forwarded to the Director, DSO, NSIR, and maintained with the record copy of the document.

8. Preparing Secret and Confidential Documents for Transmission

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, a document transported outside an approved building or facility to another agency by any means must be handled in accordance with this section.

(a) Preparation of Receipts

(i) The sender will complete NRC Form 126, “Classified Document Receipt” (available in the NRC Forms Library on the NRC SharePoint site). Copies of this form must be distributed according to the instructions on the form.

(ii) An individual form must be used for each addressee.

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

(b) Verification, Signature, and Return of Receipts

NRC Form 126, “Classified Document Receipt” (available in the NRC Forms Library on the NRC SharePoint site), must be used for outside transmission of classified information. For transmission of classified information within NRC facilities, an NRC Form 126 is not required.

(c) Envelopes and Wrappers

(i) A Classified document 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 of this handbook.

(ii) Inner Envelope or Wrapper

- The inner envelope should be sealed (e.g., seams taped) to indicate whether or not the envelope has been opened or otherwise tampered with.
- The inner envelope or wrapper must clearly indicate the address and name of both the sender and the intended recipient of the document. The approved address for classified mail of both the sender and intended recipient must be used. The classification must be placed at the top and bottom on the front and back of the inner envelope or wrapper.
- 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 the assemblage of the documents.
- The marking “Restricted Data” or “Formerly Restricted Data” must appear on the front and back of each inner envelope or wrapper, if appropriate.

(iii) Outer Envelope or Wrapper

- 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.
- The address for classified mail of both the sender and intended recipient must be used. Under no circumstances should the name of the sender or intended recipient appear on the outer envelope.

(iv) Evidence of Tampering

If the envelope or wrapper used to transmit a classified document indicates any evidence of tampering, the recipient must preserve the envelope or wrapper as received and immediately notify DFS, ADM; DSO, NSIR; those personnel responsible for the security functions in the recipient's office; and the NRC Office of the Inspector General (OIG).

9. Classified Documents from Other Agencies

(a) Safeguards to be Afforded

Documents from other agencies must be controlled, handled, marked, and safeguarded with at least those precautions prescribed for documents of the

same classification level originated by the NRC (see MD 12.1 for the physical protection requirements for classified information).

(b) Third Agency Rule

(i) The "Third Agency Rule" provides that "classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information" (see E.O. 13526, Section 4.1(i)). A document created prior to June 25, 2010 (effective date of E.O. 13526), must not be disseminated outside of the NRC without the consent of the originating agency.

(ii) For the purposes of the "Third Agency Rule," U.S. entity includes—

- State, local, or tribal governments;
- State, local, or tribal law enforcement and firefighting entities;
- Public health and medical entities;
- Regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or
- Private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(c) Registered Documents

On occasion, an NRC employee or an NRC contractor will receive a document originated by DoD personnel that is numbered and contains the notation on the cover "Registered Document," "Serial Document," or a similar designation. In these cases, an NRC employee or and NRC contractor must comply with the inventory and reporting requirements established by the originating agency. NRC employees and contractors are to consult DSO, NSIR, regarding these requirements.

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

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

10. Destruction of Secret and Confidential Documents

    (a) Responsibilities

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

    (b) Method of Destruction

    (i) Secret and Confidential classified waste must be disposed of by shredding with an approved cross-cutting shredder or other approved method specified in MD 12.1.

    (ii) Before acquiring a shredder to destroy classified documents, the shredder must be approved by DFS, ADM, in accordance with the procedures set forth in MD 13.1, “Property Management.”

    (iii) At the NRC regional facilities, electronic media/equipment and microfilm/microfiche containing classified information must be provided to the Division of Resource Management and Administration (DRMA) for destruction, in accordance with MD 12.5 and CSO-STD-2004.

    (iv) At the NRC headquarters campus and all other locations, electronic media/equipment and microfilm/microfiche containing classified information must be provided to DFS, ADM, for destruction, in accordance with MD 12.5 and CSO-STD-2004.

11. Loss or Possible Compromise of Classified Information

    (a) A security incident involving the loss or possible compromise of classified information (computer security-related or physical security-related), despite the means by which it occurs, must be (within 1 hour) reported immediately to the NRC by (1) clicking on the “Report a Security Incident” button on the NRC internal Web site (found at http://www.internal.nrc.gov/), or (2) contacting the hotline on (301) 415-6666.

    (b) When a security incident involves classified information, the person or people that discover the incident (unattended document or unauthorized release of information) should immediately take possession of the document, notify their immediate supervisor or guard force member, and take steps to protect the document or information from further disclosure.

    (c) After initial report of the security incident, the affected NRC office must ensure that corrective measures are immediately taken pending the implementation of a long-term resolution.

(d) All reported security incidents will be followed up with a preliminary inquiry. Once the preliminary inquiry has been completed, a preliminary inquiry report will be forwarded to the appropriate NRC office for action. Referrals to OIG and OIG's associated investigative role are unaffected by this MD policy.

(e) Since information about a security incident may contain classified information, all personnel are required to discuss, document, or otherwise process incident information in accordance with the appropriate classification guide, where applicable, and NRC MDs. Specifically, when communicating about security incidents involving the loss or possible compromise of classified information to other staff, management, or both, as appropriate, personnel must ensure the content of e-mail communications does not include classified information. Additionally, personnel must ensure the location of verbal communications related to security incidents (if e-mail communication is not appropriate) is cleared to a level commensurate to or higher than the level of the information being discussed, to ensure the loss or possible compromise is not further complicated by such communications. The safeguarding of documents, media, or both, related to security incidents, to include printed copies of e-mails and hand-written documents must be conducted in accordance with the physical protection requirements for classified information outlined in MD 12.1.

(f) In some instances a security incident may involve the release of classified information into the public domain. The fact that classified information appears in the public domain is in itself classified information within Government channels that must be protected at the same level as the classified information in question. In addition, the fact that classified information appeared in the public domain does not make it unclassified information. It is the policy of the NRC to neither confirm nor deny that information appearing in the public domain is or is not classified information. Any questions that are raised about the accuracy, sensitivity, or technical merit of the information should be responded to with "no comment."

(g) All security incidents involving classified information will be coordinated with DSO, NSIR, as appropriate. This coordination may be necessary to assure an accurate determination of the classification level and classification category of information. If a security incident involves classified information that originated at another agency, DFS, ADM, in consultation with DSO, NSIR, will 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.

D. Classification Guides

In accordance with E.O. 13526, Section 2.2, classification guides are required for the classification of NSI. There are also classification guides for RD and FRD.

1. Program Classification Guides

   (a) Within the NRC, program classification 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, DSO, NSIR, is responsible for issuing and revising these guides. A program guide establishes an authoritative frame of reference within which more detailed local classification guides may be prepared.

   (b) If no program classification guide applies to a specific topic, DSO, NSIR, in conjunction with appropriate offices and regions, may determine that a program classification guide needs to be developed to apply classification policy in a particular field of work. Alternatively, DSO, NSIR, in conjunction with the appropriate offices and regions, may determine that an existing program classification guide requires revision. In either instance, DSO, NSIR, will coordinate the development or revision of the program classification guide with appropriate NRC offices and regions and with other agencies, as required.

2. Approval of Guides

   The Director, DSO, NSIR, will approve each classification guide in writing. Any program guide that could affect major NRC policy decisions, as determined by the Director, DSO, NSIR, will be forwarded to the Commission for review and approval before being issued.

3. Review of Guides

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

4. Dissemination of Guides

   DSO, NSIR, will distribute classification guides as widely as necessary to ensure the proper and uniform derivative classification of information. Classification guides will be distributed in paper copies and in electronic format, when available.

5. Content of Guides

   At a minimum, classification guides should—

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

   (b) Provide the date of issuance or last review;

   (c) State precisely the elements of information to be protected, indicate which classification level applies to each element of information, and specify the elements that are unclassified;

   (d) State special handling caveats;

   (e) Prescribe a specific declassification instruction (i.e., date or event);

   (f) Specify the exemption category identified in E.O. 13526, Section 3.3(b), if any; and

   (g) State a concise reason for classification.

E. Classified Information Self-Inspections

Classified information self-inspections are conducted by DSO, NSIR, to review the classification, downgrading, and declassification practices and procedures of the headquarters offices, the regional facilities, the Technical Training Center, and the resident inspector office at each participating reactor and nuclear facility site that possess classified information to determine the accuracy and uniformity of interpretation and implementation of NRC policy and standards. DSO, NSIR, has self-inspection guidance for the standard format used for classified information self-inspections.

1. Frequency of Self-Inspections

   Classified information self-inspections are ongoing and conducted at least annually in accordance with 32 CFR Section 2001.60(d). The Director, DSO, NSIR, determines the self-inspection coverage requirements based on program and policy needs.

2. Reports

   (a) A written report must be prepared after each self-inspection that details the criteria evaluated and recommendations provided during the self-inspection.

   (b) Normally, the self-inspection results will be discussed with management personnel of the appraised organization before the final report is completed. 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.

(c) Copies of the findings and recommendations from the self-inspection will be furnished to the regional office, the headquarters office, the contractor, or other appraised organization no later than 30 calendar days after a self-inspection is completed at a given office or facility.

(d) 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. DSO, NSIR, must be provided written confirmation that the necessary corrective measures have been taken within 30 calendar days after receiving the self-inspection report.

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

1. The National Industrial Security Program Operating Manual (NISPOM), Incorporating Change 1, dated March 28, 2013 (available at http://www.dss.mil/isp/fac_clear/download_nispom.html), implements the provisions of E.O. 12829, "National Industrial Security Program." A company is considered to be under foreign ownership, control, or influence (FOCI) whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or otherwise, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified information contracts. Upon receiving indication that a potential NRC contractor requires access to classified information (as evidenced by designation under block 5 of the NRC Form 187, "Contract Security and/or Classification Requirements" (available in the NRC Forms Library available at http://portal.nrc.gov/nrcformsportal/default.aspx on the NRC SharePoint site), the Acquisition Management Division (AMD), ADM, will forward the NRC Form 187 and Statement of Work to DFS, ADM, to determine whether or not a reasonable basis exists for concluding that a compromise or an unauthorized disclosure of classified information may occur.

2. 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.

3. DFS, ADM, will consider the following factors to determine whether a company is under FOCI, is eligible for an FCL, and the protective measures required—

   (a) Foreign intelligence threat;

   (b) Risk of unauthorized technology transfer;

   (c) Type and sensitivity of the information requiring protection;

   (d) Nature and extent of FOCI, including whether a foreign person occupies a controlling or dominant minority position, and the source of FOCI, including identification of immediate and ultimate parent organizations;

   (e) Record of compliance with pertinent U.S. laws, regulations, and contracts; and

   (f) Nature of bilateral and multilateral security and information exchange agreement.

4. DFS, ADM, may require a contractor being assessed for FOCI to provide information concerning—

   (a) Direct or indirect ownership of 5 percent or more of the applicant company's voting stock by a foreign person.

   (b) Direct or indirect ownership of 25 percent or more of any class of the applicant company's nonvoting stock by a foreign person.

   (c) Management positions, such as directors, officers, or executive personnel of the applicant company, held by other than U.S. citizens.

   (d) 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.

   (e) Contracts, agreements, understandings, or arrangements between the applicant company and a foreign person.

   (f) Details of loan arrangements between the 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.

   (g) Total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign people in the aggregate.

   (h) 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.

(i) Interlocking directors with foreign people and any officer or management official of the applicant company who is also employed by a foreign person.

(j) Any other factor that indicates or demonstrates a capability on the part of foreign people to control or influence the operations or management of the applicant company.

(k) Ownership of 10 percent or more of any foreign interest.

5. If an applicant company provides information that would indicate FOCI concerns, DFS, ADM, will review the case to determine the relative significance of the information relative to the factors listed under Sections I.F.3–4 above, the extent to which FOCI could result in unauthorized access to classified information, and the type of actions necessary to reduce the effects of FOCI to an acceptable level. However, if DFS, ADM, determines a company is under FOCI and that the appropriate methods are not applied to negate or mitigate the risk of FOCI, DFS, ADM, will suspend the FCL.

II. SPECIAL HANDLING OF CLASSIFIED INFORMATION

A. Control of Top Secret Documents

1. The following requirements pertain to Top Secret collateral documents and information. Other classified documents requiring special handling will be handled in accordance with the “U.S. NRC Sensitive Compartmented Information Facility (SCIF) Security Guide and Standard Operating Procedure (SOP),” which is maintained by the Central Top Secret Control Officer (CTSCO) in ISB, DSO, NSIR.

2. 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.

3. Access Lists

(a) Access to Top Secret information, including Top Secret National Security Council Information (NSCI), requires a "Q" clearance, a need-to-know, and the written authorization of the regional administrator or the director of the office sponsoring the activity or in which the individuals seeking access are employed.

(b) Each region and office with personnel authorized access to Top Secret information, including Top Secret NSCI, will maintain a list of its authorized personnel. A copy of the access list for each region and office must be provided to DSO, NSIR.

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

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

4. Sanctions

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

(i) Knowingly, willfully, or negligently disclose to an unauthorized person, information properly classified under E.O. 13526, predecessor E.O.s, or the AEA.

(ii) Knowingly and willfully classify or continue the classification of information in violation of E.O. 13526, or any implementing directive.

(iii) Knowingly and willfully violate any other provision of E.O. 13526, or any implementing directive, or the AEA relating to the classification and declassification of RD and FRD.

(b) 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.

5. Central Top Secret Control Officer and Top Secret Control Officers

The following requirements pertain to paper copies of documents and except where explicitly stated, the following requirements are not applicable to electronic documents. However, once electronic documents are printed, they must meet the requirements of this section.

(a) Central Top Secret Control Officer

(i) The Director, DSO, NSIR, has assigned central control functions for Top Secret information to ISB, DSO, NSIR, and has appointed a CTSCO and designated alternates from ISB, DSO, NSIR, to ensure efficient operation of the central control functions for Top Secret information. These functions include assigning control numbers and, when applicable, series designators for all Top Secret documents, as well as accountability and inventory responsibilities.

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

- A Top Secret document originated by the NRC or its contractors working in the headquarters area must be delivered immediately to the CTSCO. (Authority to originally classify an NRC document or NRC contractor document at the Top Secret level is limited to the Commissioners, the EDO, and the DEDR.)
- A Top Secret document received from another agency by the NRC or an NRC contractor in the headquarters area must be delivered immediately to the CTSCO.
- A Top Secret document originated by an approved NRC regional office or an NRC contractor outside the headquarters area, or received from another agency, must immediately be 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.

(b) Top Secret Control Officers

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

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

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

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

6. Accountability Control Files

(a) The following requirements pertain to paper copies of documents and, except where explicitly stated, are not applicable to electronic documents. However, once electronic documents are printed, they must meet the requirements of this section.

(b) 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:

(i) Document Register

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

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

(iii) Document title or subject;

(iv) Date of document;

(v) Date of receipt or origination;

(vi) Originating NRC office, NRC contractor, or outside agency; and

(vii) Classification and category (NSI, RD, FRD) and control caveats.

(c) Receipt File

The receipt file is a record of the NRC Forms 126 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 DSO, NSIR.

(d) Document History File

The document history file contains a copy of NRC Form 126 for Top Secret documents forwarded to another agency and copies of NRC Form 124, "Top Secret Access Log" (this form can be obtained from the CTSCO in DSO, NSIR) 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).

7. Assignment of a Control Number to Documents From Other Agencies

(a) The following requirements pertain to paper copies of documents and except where explicitly stated, the following requirements are not applicable to electronic documents. However, once electronic documents are printed, they must meet the requirements of this section.

(b) The CTSCO assigns a unique NRC control number to each Top Secret document received by the 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.

8. Physical Inventory

The following requirements pertain to paper copies of documents and except where explicitly stated, the following requirements are not applicable to electronic documents. However, once electronic documents are printed, they must meet the requirements of this section.

(a) Top Secret documents under the control of the CTSCO, and Top Secret documents in the custody of authorized recipients, must be inventoried annually under the direction of the CTSCO. This inventory must be completed by July 31 of each year.

(b) The CTSCO will initiate the inventory and prepare an inventory record listing of Top Secret documents from the accountability control files. The following identification will be provided for each Top Secret document—

(i) Control number,

(ii) Abbreviated title or subject,

(iii) Copy number and series,

(iv) Document date,

(v) Date of transfer to the authorized holder, and

(vi) Name of the person who currently is assigned custody of the document.

(c) The CTSCO will forward the inventory record listing of Top Secret documents to those people who currently are assigned custody of Top Secret documents. Each custodian must physically account for each document in his or her possession 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 in his or her custody, the custodian will sign and date the inventory record listing and return it to the CTSCO on or before the specified completion date.

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

(i) NRC Form 124 must be signed by each person who has access to the document.

(ii) NRC Form 126 must be used when transmitting a Top Secret document to authorized custodians.

(iii) Standard Form 703, "Top Secret Cover Sheet" (available in the NRC supply room at headquarters and in each region), 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 the NRC, NRC contractors, 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.

9. Reproduction of Top Secret Documents

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

(b) Reproduction of Top Secret documents must be completed in accordance with MD 12.5.

(c) To reproduce a Top Secret document, the originator of the Top Secret document, after consultation with the CTSCO, will deliver the document to the CTSCO, who will reproduce the number of copies required for distribution.

(d) Subsequent reproduction of a Top Secret document (e.g., Series B, C, D) after the original set will be authorized only in an extreme emergency. When there is an emergency, a written request describing the circumstances that justify reproduction must be submitted to the Director, DSO, NSIR.

(e) If the request is approved, the CTSCO will reproduce the document. The CTSCO will assign the copy the next series designator (e.g., B, C, D, etc.) and record all pertinent information required in Sections II.A.5 – 6 of this handbook. The requester will ensure that the following statement is placed on the upper right side of the copy underneath the existing documentation and that it is accurately completed:

"Series _____Copy_____ of_____copies."

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

(g) If the request is disapproved, the Director, DSO, NSIR, will advise the requester in writing.

10. Reproduction of Top Secret Documents from Other Agencies

    A Top Secret document or portion of a document 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 must obtain written approval from the agency involved. Upon receipt of this approval, the individual will request that the CTSCO reproduce the information in accordance with Section II.A.7 of this handbook and MD 12.5.

11. Transmission of Top Secret Documents

    (a) A Top Secret document may only be transmitted by approved means. These approved means include the Defense Courier Service, hand-carried by specifically authorized NRC employees and NRC contractors, and electronically transmitted through an appropriately encrypted telecommunication circuit. Transmission of classified information in ADAMS or in the Electronic Information Exchange is prohibited. Procedures applicable to handling classified messages within approved communications centers are set forth in MD 12.4 and MD 12.5. Under no circumstances may Top Secret documents be transmitted through the U.S. Mail or an NRC or NRC contractor internal mail service.

    (b) Top Secret information must be transmitted, to the maximum extent possible, by a discussion between authorized people in an area prescribed by the Director, DSO, NSIR, or by secure communications approved by the Director, DSO, NSIR. Otherwise, Top Secret information must be hand-delivered by an authorized person within the same building, or by an NRC authorized courier or the Defense Courier Service, when Top Secret information must be delivered to another building, facility, or Government agency. A person hand-carrying a Top Secret document must keep the document continuously in his or her possession until the information is stored in an approved facility or is turned over to a designated recipient.

    (c) Before transmitting, including electronic transmission, or transferring any Top Secret document, the CTSCO must be consulted. Approval for an NRC contractor employee to hand-carry a classified document during travel by a commercial airline must be obtained from the Director, DSO, NSIR. Additionally, the Transportation Security Administration (TSA) screens travelers and matter transported by air in accordance with U.S.C. 49, “Transportation,” Chapter 449, “Security.”

12. Receipts

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

13. Destruction of Top Secret Documents

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

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

B. Naval Nuclear Propulsion Information

1. U.S. naval nuclear propulsion information may be either classified or unclassified information. It must be made available on a need-to-know basis only to appropriately cleared (“L” or “L(H)” clearance for access up to Secret NSI and “Q” clearance for access to Secret Restricted Data (SRD) and above) NRC employees and NRC contractors who are U.S. citizens. Further explanation of the applicable clearances needed to access U.S. naval nuclear propulsion information can be found in MD 12.3, "NRC Personnel Security Program."

2. 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, DOE, with an information copy to DSO, NSIR. DSO, NSIR, is also available to provide assistance.

3. Public release of classified and unclassified naval nuclear propulsion information, or foreign release thereof, is not permitted. Any FOIA request from a source outside the NRC for nuclear propulsion documents or information must be forwarded through the Office of Information Services (OIS) to the Office of Naval Reactors, DOE, for disposition.

4. Classified naval nuclear propulsion information and documents must be protected and handled in accordance with existing security directives. Storage and dissemination of classified or unclassified naval nuclear propulsion documents in ADAMS is prohibited.

5. 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 the following marking:

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

C. National Security Council Information (NSCI)

1. Responsibilities

   (a) All classified NSCI documents must be controlled, handled, marked, and protected in accordance with Sections I.B - C of this handbook (see MD 12.1 for the physical protection requirements for classified information).

   (b) Access to classified NSCI must be limited to the absolute minimum number of NRC employees and NRC contractors holding the requisite clearance, who have a need-to-know, and who require such access to perform their official duties (see MD 12.3, Exhibit 4, for Security Clearance/Access Types). National Security Decision Directive 19 (NSDD-19), "Protection of Classified National Security Council and Intelligence Information," provides the basis for limiting the number of NRC employees and NRC contractor personnel with access to National Security Council matters to the minimum consistent with operational requirements and needs.

   (c) NRC employees and NRC contractors must observe and respect all enhanced control, handling, marking, and protection requirements for classified NSCI imposed by the National Security Council.

2. Requirements

   (a) Receipt and Handling

      (i) All classified NSCI transmitted to the NRC by the National Security Council will be addressed to the Chairman and received by SECY. Classified NSCI electronically transmitted to the NRC will be received by an approved communications center and a paper copy of the transmission will be delivered to SECY.

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

(iii) Upon receipt of NSCI, SECY will forward the NSCI document to the responsible individual(s) designated on the intended recipient's access list.

(iv) If the NSCI document is to be distributed at the staff level, the Technical, Corporate, and Correspondence Management Branch, OEDO, will forward the NSCI document to the responsible individual(s) at the staff level designated on the intended recipient's access list.

(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, ADM, staff, who will conduct an inquiry into the matter and take the necessary action to prevent recurrence.

(b) Reproduction

(i) A document 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.

(ii) Reproduction of a classified document containing NSCI must be completed in accordance with MD 12.5.

(c) Documents Generated by NRC

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

(d) Loss or Possible Compromise of Documents

(i) A security incident involving the loss or possible compromise of classified NSCI (computer security-related or physical security-related), despite the means by which it occurs, must be reported immediately (within 1 hour) to the NRC by (1) clicking on the “Report a Security Incident” button on the NRC internal Web site, or (2) contacting the hotline on (301) 415-6666.

(ii) When a security incident involves classified information, the person or people that discover the incident (unattended document or unauthorized release of

information) should immediately take possession of the document, notify their immediate supervisor or guard force member, and take steps to protect the document or information from further disclosure.

(iii) After initial report of the security incident, the affected NRC office must ensure that corrective measures are immediately taken pending the implementation of a long-term resolution.

(iv) All reported security incidents will be followed up with a preliminary inquiry. Once the preliminary inquiry has been completed, a preliminary inquiry report will be forwarded to the appropriate NRC office for action. Referrals to OIG and OIG's associated investigative role are unaffected by this MD policy.

(v) A written report on the matter, including corrective measures taken, where appropriate, will be submitted by the EDO or the responsible Commission office to the Chairman.

(vi) Since information about a security incident may contain classified information, all personnel are required to discuss, document, or otherwise process incident information in accordance with the appropriate classification guide, where applicable, and NRC MDs. Specifically, when communicating about a security incident involving the loss or possible compromise of classified information to other staff, management, or both, as appropriate, personnel must ensure the content of e-mail communications does not include classified information. Additionally, personnel must ensure the location of verbal communications related to security incidents (if e-mail communication is not appropriate) is cleared to a level commensurate to or higher than the level of the information being discussed to ensure the loss or possible compromise is not further complicated by such communications. The safeguarding of documents, media, or both, related to security incidents, including printed copies of e-mails and hand-written documents, must be conducted in accordance with the physical protection requirements for classified information outlined in MD 12.1.

(vii) In some instances a security incident may involve the release of classified information into the public domain. The fact that classified information appears in the public domain is in itself classified information within Government channels that must be protected at the same level as the classified information in question. In addition, the fact that classified information appeared in the public domain does not make it unclassified information. It is the policy of the NRC to neither confirm nor deny that information appearing in the public domain is or is not classified. Any questions raised about the accuracy, sensitivity, or technical merit of the information should be responded to with "no comment."

(viii) All security incidents involving classified NSCI will be coordinated with DSO, NSIR, as appropriate. This coordination may be necessary to assure an accurate determination of the classification level and classification category of information. If a security incident involves classified NSCI, DFS, ADM, in consultation with DSO, NSIR, will notify the National Security Council so that a damage assessment can be conducted and appropriate measures taken to negate or minimize any adverse effect.

(e) Classification, Declassification, or Downgrading

Any classification, declassification, or downgrading questions on NSCI must be referred to DSO, NSIR.

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

SECY, in consultation with the Office of the General Counsel (OGC), will determine what NSCI records, if any, are subject to the FOIA. OIS must be notified when NSCI records are the subject of a FOIA request. OIS will be responsible for referring the records to the National Security Council.

D. Transfer of Classified Information to Foreign Governments and International Organizations

1. Authorities

(a) Classified Nonmilitary Information

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.

(b) Classified Military Information

Basic policy governing the release and disclosure of classified military information is specified in National Disclosure Policy-1, "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 United States Military Information to Foreign Governments and International Organizations."

(c) Restricted Data and Formerly Restricted Data

The provisions of Section II.D of this handbook do not apply to the transmission of RD or FRD to foreign governments or international organizations. RD and FRD

are furnished to and received from foreign governments and international organizations only in accordance with agreements for cooperation negotiated in the provisions of Sections 123 and 144 of the AEA.

(d) Prohibitions on Disclosure

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

2. Criteria

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

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

(i) A determination must be made for the following:

- Whether the required General Security Agreement is in effect with the country and, if not, whether an exemption/waiver has been granted or should be sought from the U.S. Secretary of State;
- Whether an agency-to-agency level agreement to exchange classified information is in place and, if not, how to seek a waiver from the Commission; and
- Whether this is the first or a subsequent request for the release of classified NRC information to that country.

(ii) A determination that a need-to-know exists, and that the furnishing of classified information will result in a net advantage to the national security interests of the United States, must be made by the Director, Office of International Programs (OIP). In making this determination, disclosure is—

- Consistent with the foreign policy of the U.S. toward the recipient government.
- Consistent with the policies of the U.S. Government with regard to the AEA, the ERA, or with regard to information for which special procedures for release have been or may hereafter be established by competent authority having statutory jurisdiction over the subject matter.
- Consistent with the national security interests of the U.S.

- Limited to information necessary to the purpose for which disclosures are made.

(iii) The recipient government must have agreed, either generally or in the particular case, to—

- Not release the information to a third party without the approval of the releasing party.
- Afford the information substantially the same degree of protection afforded it by the releasing party.
- Not use the information for other than the purpose for which it was given.
- Respect rights such as patents, copyrights, or trade secrets in the event that the releasing party indicates private rights are involved in the information.

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

(i) 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 II.D.2(a) of this handbook. 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.

(ii) The Commission has determined that the release of classified information to the IAEA, as agreed upon by the Agreement Between The United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto) (U.S./IAEA Safeguards Agreement) will result in a net advantage to the national security interest of the U.S. Furthermore, Article 5 of the U.S./IAEA Safeguards Agreement satisfies the criteria of Section II.D.2(a) of this handbook. The criteria of Section II.D.2(a) of this handbook have been waived by the Commission.

3. Responsibilities

(a) After it is determined that the requesting organization has a need-to-know, the Director, OIP, will determine whether or not furnishing classified information will result in a net advantage to the national security interests of the U.S. The determination must be made with the concurrence of OGC, DSO, NSIR, and the responsible program office. OIP will consult with the U.S. 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. OIP will send a request to the Commission for permission to share classified information for each request, listing the information to be shared, the timing of the proposed sharing, the recipient of the information, and the outcome of the OIP Director's net advantage determination.

(b) Classified Information Exchange Agreements with Foreign Governments

(i) Before an exchange agreement is developed, DSO, NSIR, will determine whether an applicable prerequisite government-to-government agreement exists between the U.S. and the foreign country involved.

(ii) If an agreement exists, DSO, 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.

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

(iv) The Commission will approve any waiver of the required understandings identified in Section II.D.2(a)(ii) of this handbook concerning the criteria specified. The Commission will also approve any waiver of the requirement for a separate classified exchange agreement referenced in Section II.D.3(a)(ii) of this handbook.

(v) An agreement with a foreign government will not commit the NRC to disclose any particular or specific classified information.

(c) Classified Information Exchange Agreements with International Organizations

(i) 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, DSO, NSIR, must be consulted before permitting representatives of international organizations (with the exception of the IAEA) access to classified information.

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

4. Internal Procedures

(a) Transfer of Classified Information to Foreign Governments

(i) Security Assurances

- A security assurance must be required regarding the original recipients of classified information.
- Security assurances will be obtained from an authorized person of a foreign government.
- The EDO is authorized by National Security Decision Memorandum 119 on Foreign Disclosure and SECY-78-84, “Transfer of Classified Non-military Information to Foreign Governments by NRC,” (ADAMS Accession Number ML12272A645) to waive the requirement for a security assurance for high-ranking foreign government civil or military representatives when necessary.

(ii) Review of Information to be Shared with Foreign Governments

A Classified document to be transmitted to a foreign government must be forwarded to DSO, NSIR, for review and transmission. The review must ensure that—

- Each original recipient possesses a prescribed security assurance or a waiver has been obtained.
- 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.
- OGC has concurred on the legal aspects of the transfer.

(iii) If the transfer involves a classified document or other classified information originated, produced, or received from another department or agency, DSO, NSIR, will obtain approval from this department or agency.

(iv) Classified information to be shared with foreign governments within the NRC must be coordinated with DSO, NSIR, in advance to ensure the procedures in Section II.D.4(a) of this handbook are observed.

(v) Accountability

- DSO, NSIR, and each NRC office or division proposing the release of classified nonmilitary information to a foreign government or concurring in the release must maintain a record of accountability of the information being processed for release. The record must include—
  - Identification of the exact information released or being processed for release (for documents, the date, title, name of originator, and classification);
  - Names and signatures of approving officials;
  - Form in which information is released or will be released (e.g., oral or documentary);
  - Date of release or contemplated release;
  - Identity of foreign government organization and the original individual recipient to whom release is made or is contemplated;
  - Statement that the information is based on data originated outside NRC, wherever applicable, and the identity of the originating organization; and
  - Name of individual in other U.S. Government agency who has authorized release, if applicable.
- NRC Form 126 is an acceptable record of accountability if all the required fields detailed above are included on the completed form.
- The office or division contemplating or making oral disclosures must furnish memoranda before and after these disclosures to the directors of DSO, NSIR, and OIP, and to OGC.

(vi) Preparation and Method of Transmission

The preparation (including classification) and method of transmission of documents are specified in Section I.C of this handbook. Classified information to be transmitted to foreign governments will use government-to-government mail channels. Normally, documents intended for a foreign government will be forwarded to that country's embassy in the U.S. Transmission of classified mail to foreign countries requires prior approval of the Director, DSO, NSIR.

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

The transfer of classified information to international organizations, except IAEA (see Section II.D.4 of this handbook), must be handled in accordance with guidance from DSO, NSIR.

(c) Transfer of Classified Information to IAEA

(i) Written Disclosure Authorization

- A written disclosure authorization from DSO, NSIR, is required before IAEA representatives may have access to NSI. This authorization states that the individual is an authorized IAEA representative and is authorized to make visits or inspections in accordance with the U.S./IAEA Safeguards Agreement. The authorization includes—
  - The identity of the authorized IAEA representative,
  - Specific authority to disclose NSI to that individual relating to the visit or inspection,
  - The level of classified information authorized,
  - A description of the IAEA representative's identification documents,
  - The purpose of the visit or inspection, and
  - The duration of the authorization to receive the information.
- 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.

(ii) Review of Documents to be Transferred

- Classified documents to be furnished to IAEA representatives by approved means, or transmitted to IAEA representatives, must be reviewed by DSO, NSIR, before release. The review must ensure that the information to be furnished or transmitted is within the scope of the written disclosure authorization.
- If access or transmission involves classified information originated by another department or agency, DSO, NSIR, will obtain approval from the department or agency before access or transmission.

(iii) Accountability

See Section II.D.4(a) of this handbook.

(iv) Preparation and Method of Transmission

See Section II.D.4(a) of this handbook.

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

DSO, NSIR, will report to the National Disclosure Policy Committee (NDPC) 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.

(vi) Review and Concurrence in Legal Aspects of Transfer

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

E. Classified Conferences

1. Conferences and Symposia

(a) 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.

(b) Papers involving sensitive programs or installations are to be submitted to an NRC authorized classifier (see Section I.B of this handbook) or to DSO, NSIR, for review before unclassified use.

(c) All NRC employees and NRC contractors who are to deliver briefings that involve sensitive programs or installations will have the text of such briefings reviewed for classification by an NRC authorized classifier or by DSO, NSIR, before presentation.

2. Publication or Release of Documents

When there is a doubt as to whether a document contains NSI, RD, or FRD, the author will refer the information to the appropriate NRC authorized classifier or the Director, DSO, NSIR, for a classification review.

3. Review of Documents

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 protected against unauthorized disclosure, 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 unauthorized or inadvertent disclosure in conjunction with the release of unclassified information.

4. Review of Documents Submitted by Uncleared Authors

   A document 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 DSO, NSIR, for review. If, after review, it is determined that the article contains information that should be classified, DSO, NSIR, will advise the author, to the extent possible within the bounds of security and the NRC's "No Comment" policy, of the reason for the classification and, if possible, take action to have the author delete any classified information contained in the document. In the course of such a review, DSO, NSIR, will refer the document to other NRC offices, to the NRC regions, and to other Government agencies, as appropriate.

5. Review of Documents Submitted by Formerly Cleared People or by Authors with Active Clearances

   A document submitted by a person formerly cleared at the "Q," "L(H)," or "L" level, by a person with an active NRC clearance other than someone set forth in MD 12.3 or by a person formerly or currently cleared by another Government agency must be reviewed by an NRC authorized classifier or by DSO, NSIR. The author is required to delete any classified information in the document before it is published.

F. Hand-carrying Classified Material

1. Authority to Hand-carry Classified Material

   (a) An authorized person hand-carrying classified information (Secret or below) outside the protective controls of an NRC facility, licensee, or other Government agency for return to the protective controls of an NRC facility, licensee, or other Government agency, regardless of the duration or distance of the trip, must obtain authorization from the Director, DFS, ADM, or a designated alternate identified in writing by the Director, DFS, ADM, in the form of a courier letter or courier card.

(b) Within the NRC headquarters campus, the One White Flint North, Two White Flint North, and Three White Flint North buildings are co-located on one campus and personnel transporting classified information (Secret or below) are not required to possess a courier card or courier letter when transporting classified information on foot between facilities. Transporters of classified information (Secret or below) must adhere to the guidance stated in Sections I.C.1–8 of this handbook.

2. Courier Letters

A letter of Courier Authorization from the Director, DFS, ADM, or a designated alternate identified in writing by the Director, DFS, ADM, is required when hand-carrying classified information (Secret or below) is deemed necessary. The authorized person must also sign a courier procedures agreement in the presence of the issuing official. A new authorization letter is required for each period of courier activity.

3. Courier Card

A courier card from the Director, DFS, ADM, or a designated alternate identified in writing by the Director, DFS, ADM, is issued instead of a courier letter for those authorized people who handle and transport classified material (Secret or below) on a regular basis. When no longer needed, the card will be returned to the issuing office, which will hold the card until it is needed or it expires.

G. Transporting Classified Material by Commercial Airlines

1. Approval for an NRC employee or an NRC contractor to hand-carry classified documents during travel by commercial airlines must be obtained from the Director, DFS, ADM. In addition, TSA has issued regulations for screening travelers and matter transported by air. Accordingly—

(a) Each NRC employee and NRC contractor employee hand-carrying classified information must carry his or her travel authorization and his or her NRC identification badge that has his or her photograph on it. The employee must also carry the document authorizing him or her to hand-carry the information.

(b) TSA requires all passengers and items transported be screened before boarding an aircraft. Briefcases or other luggage, including those containing 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.

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

(d) When the classified documents to be transported are of a size, weight, or shape not suitable for the processing specified above, the following procedures apply:

(i) An NRC employee or an NRC contractor who has 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.

(ii) An employee carrying a classified package must report to the airline ticket counter and present documentation and a description of the containers that are exempt from screening.

(iii) An employee must have the original correspondence signed by appropriate supervisory personnel authorizing him or her to carry classified documents. This correspondence must be prepared on NRC letterhead stationery or the stationery of the contractor employing the individuals.

(iv) An employee must have enough authenticated copies of this correspondence to provide a copy to each airline involved.

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

(a) The full name of the employee and the NRC office or the NRC contractor by whom he or she is employed.

(b) A description of the type of identification the employee will present (e.g., NRC photo badge).

(c) 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.

(d) Identification of the point of departure, destination, and known transfer points.

(e) Date of issue and the expiration date of the correspondence, which is not to exceed 7 days from the date of issue.

(f) Name, title, signature, and telephone number of official authorizing the employee to carry the classified documents.

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

3. 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 a classified package on a return trip and the letter from his or her organization does not cover this return trip, a letter of authorization must be prepared on the letterhead stationery of the agency or the contractor being visited.

EXHIBITS

Exhibit 1 Required Markings for Classified Documents

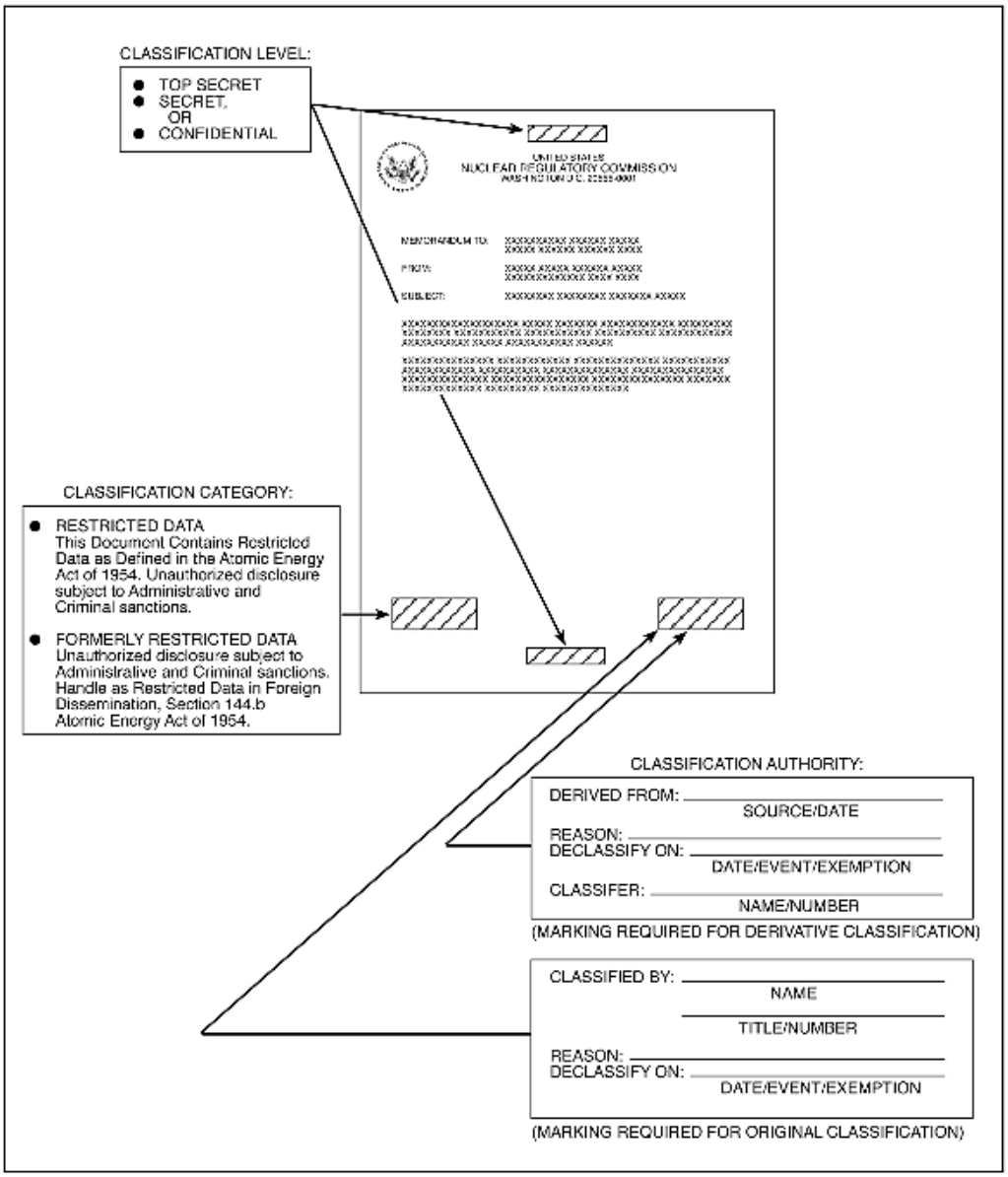


Exhibit 2 Declassification Markings

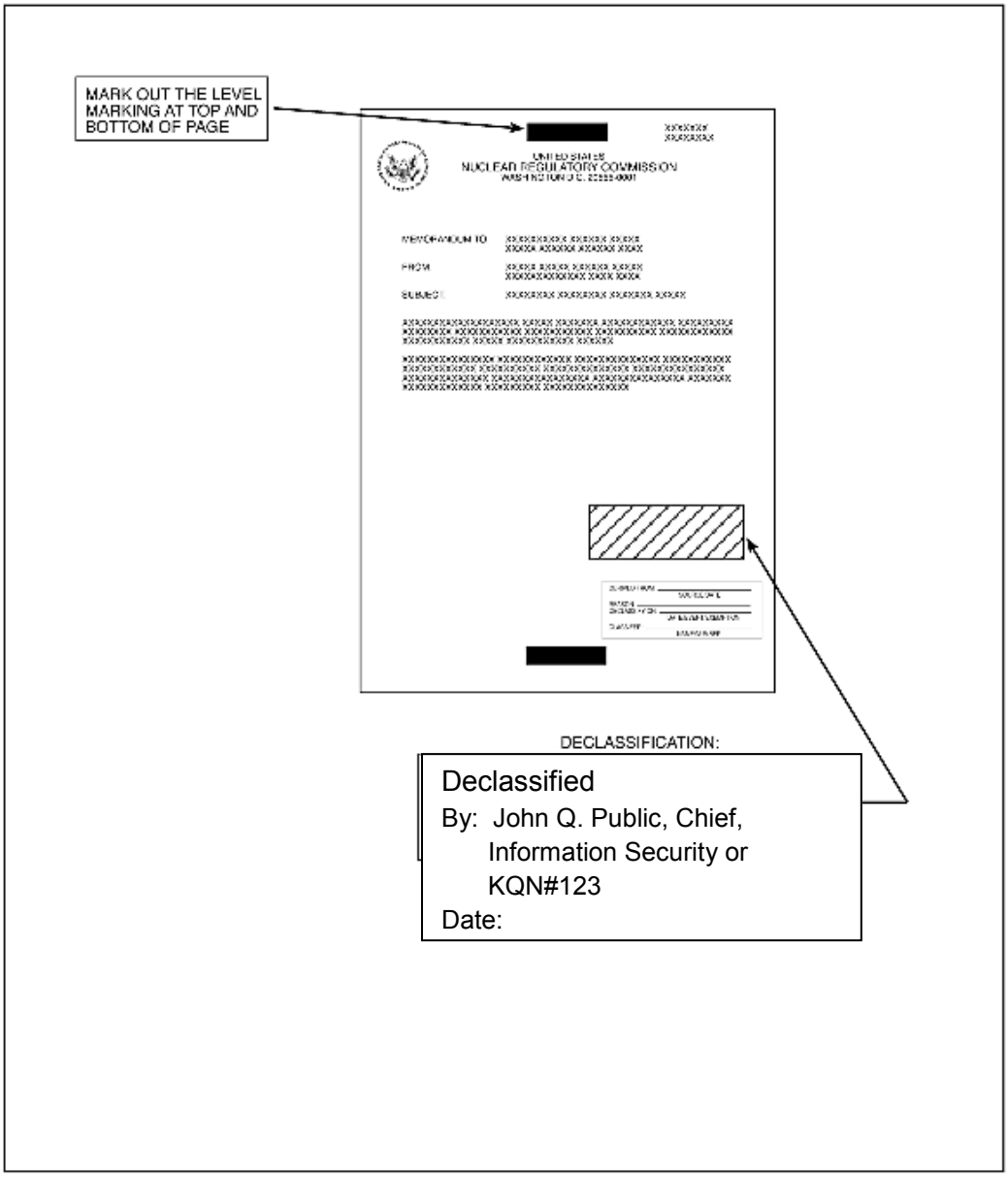


Exhibit 3 Subject or Title Marking and Portion-Marking

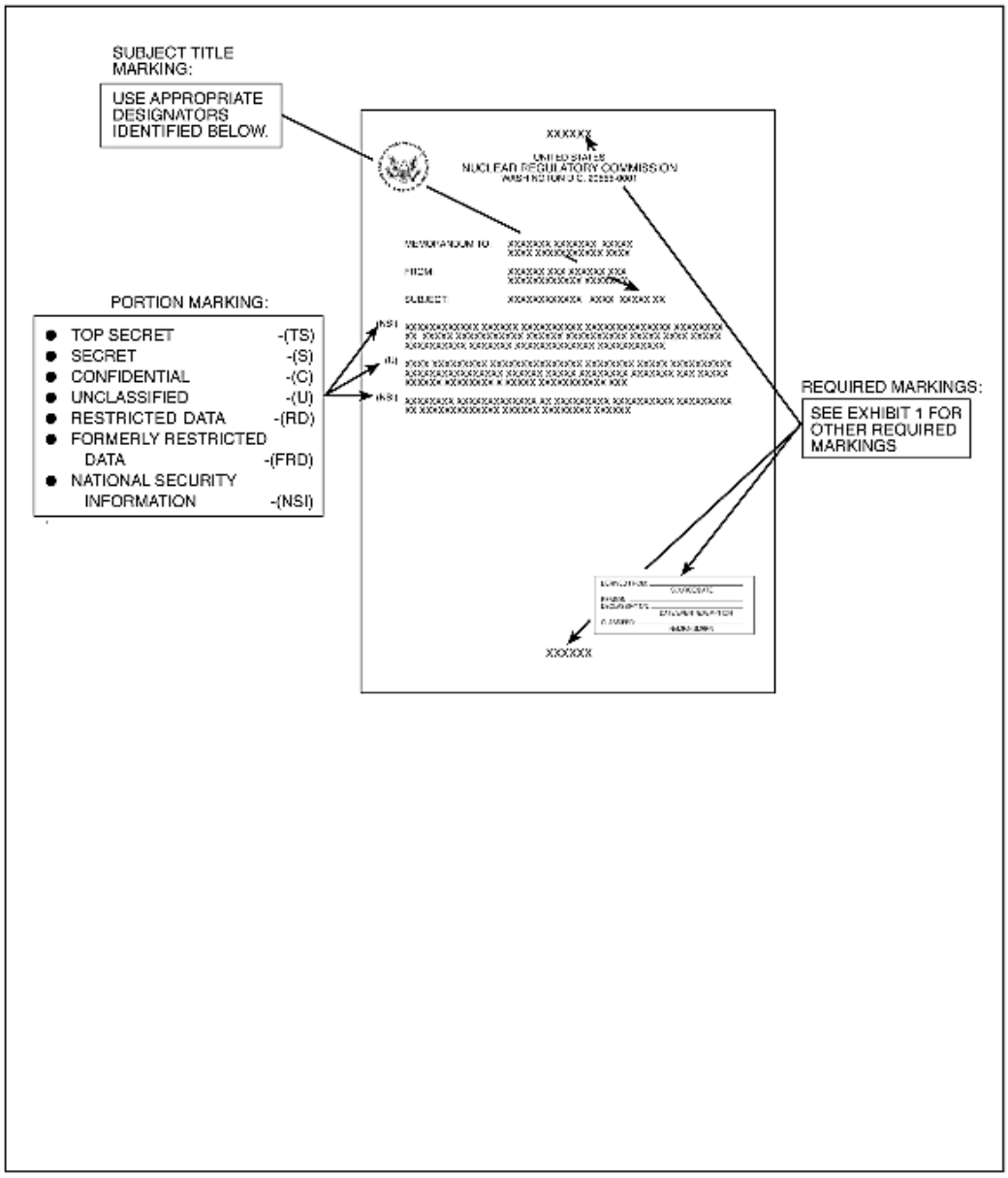


Exhibit 4 Upgrading, Downgrading, and Transclassification Markings

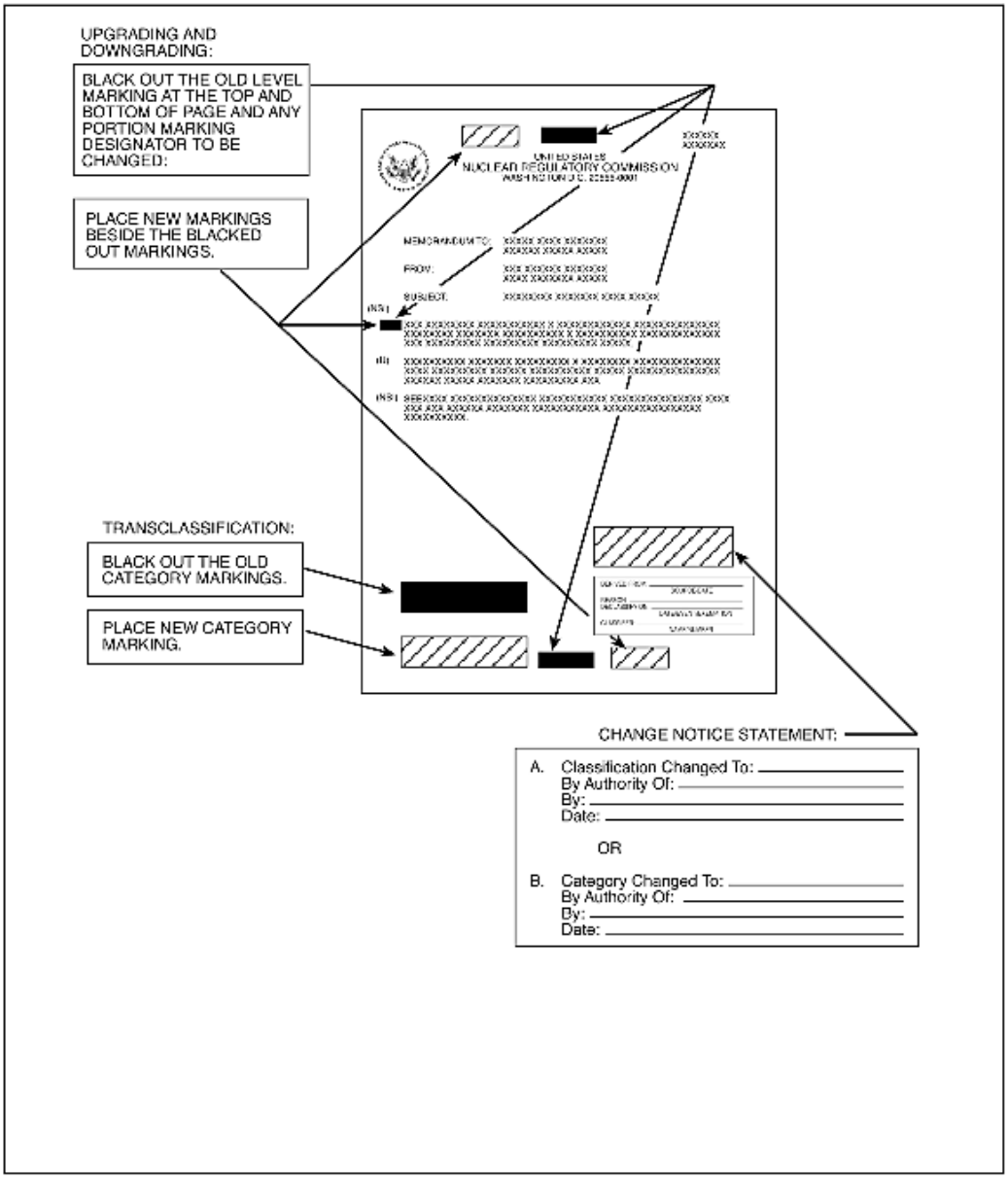


Exhibit 5 Deleting Classified Information From Classified Documents

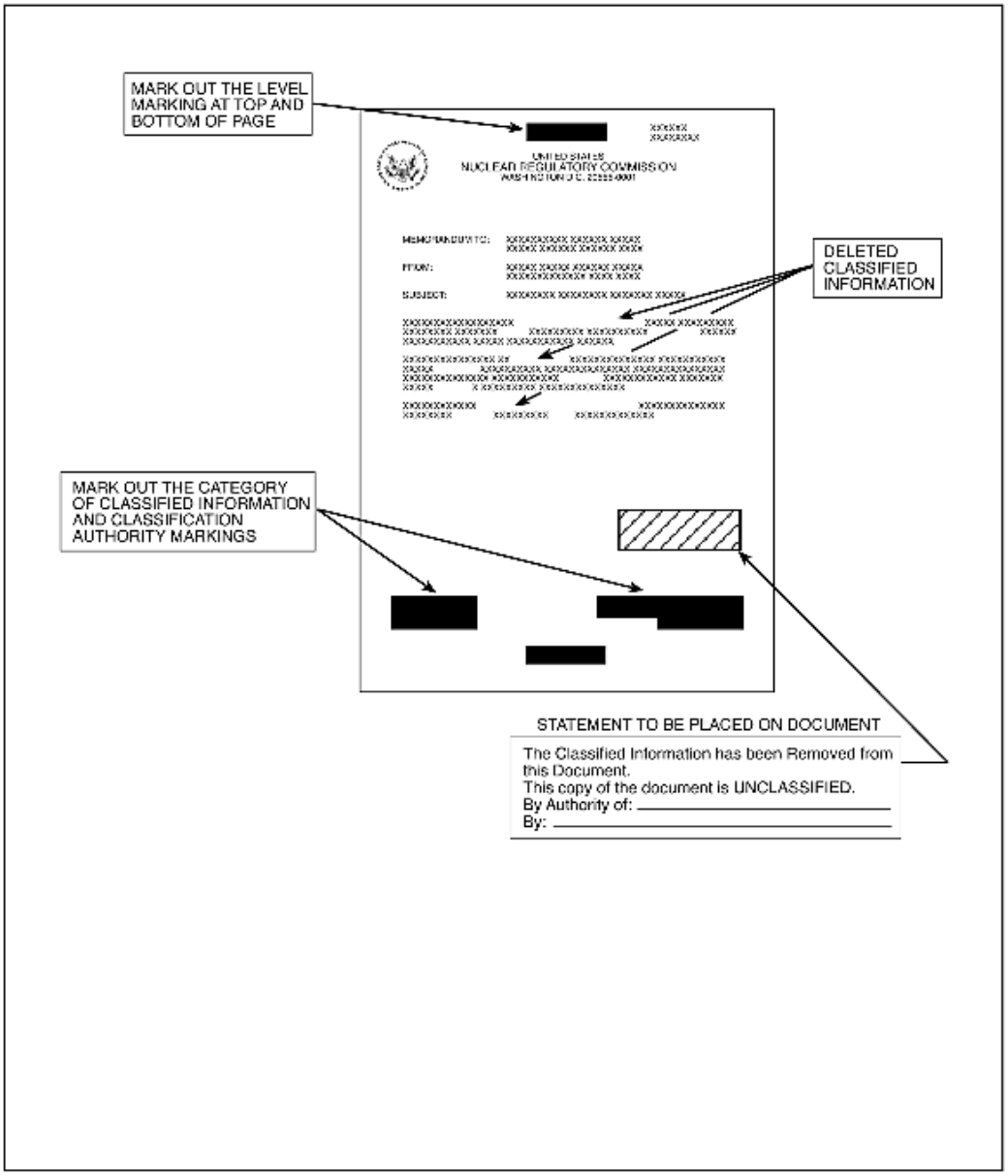


Exhibit 6 Required Markings for an Unclassified Transmittal Document

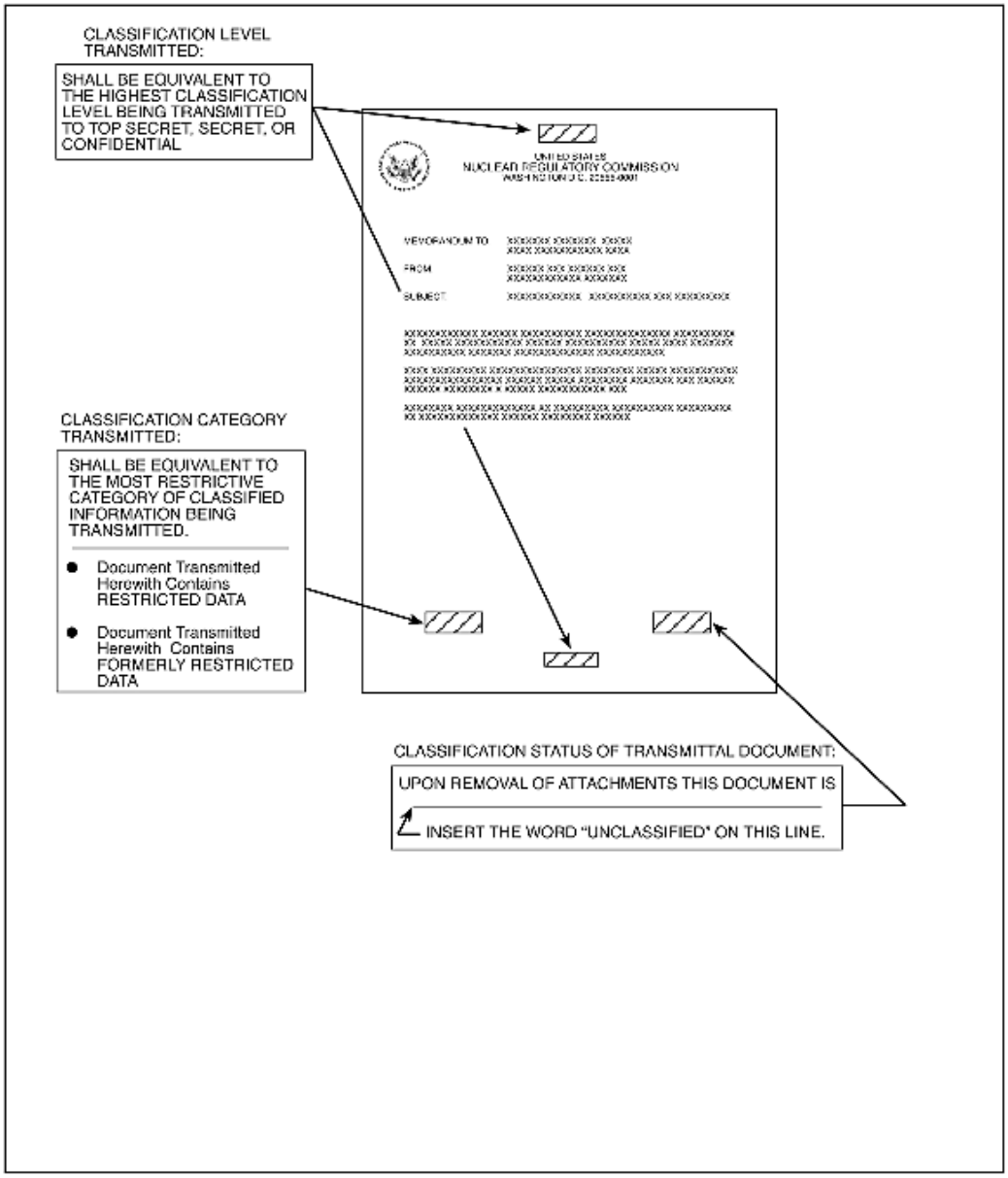


Exhibit 7 Required Markings for a Classified Transmittal Document

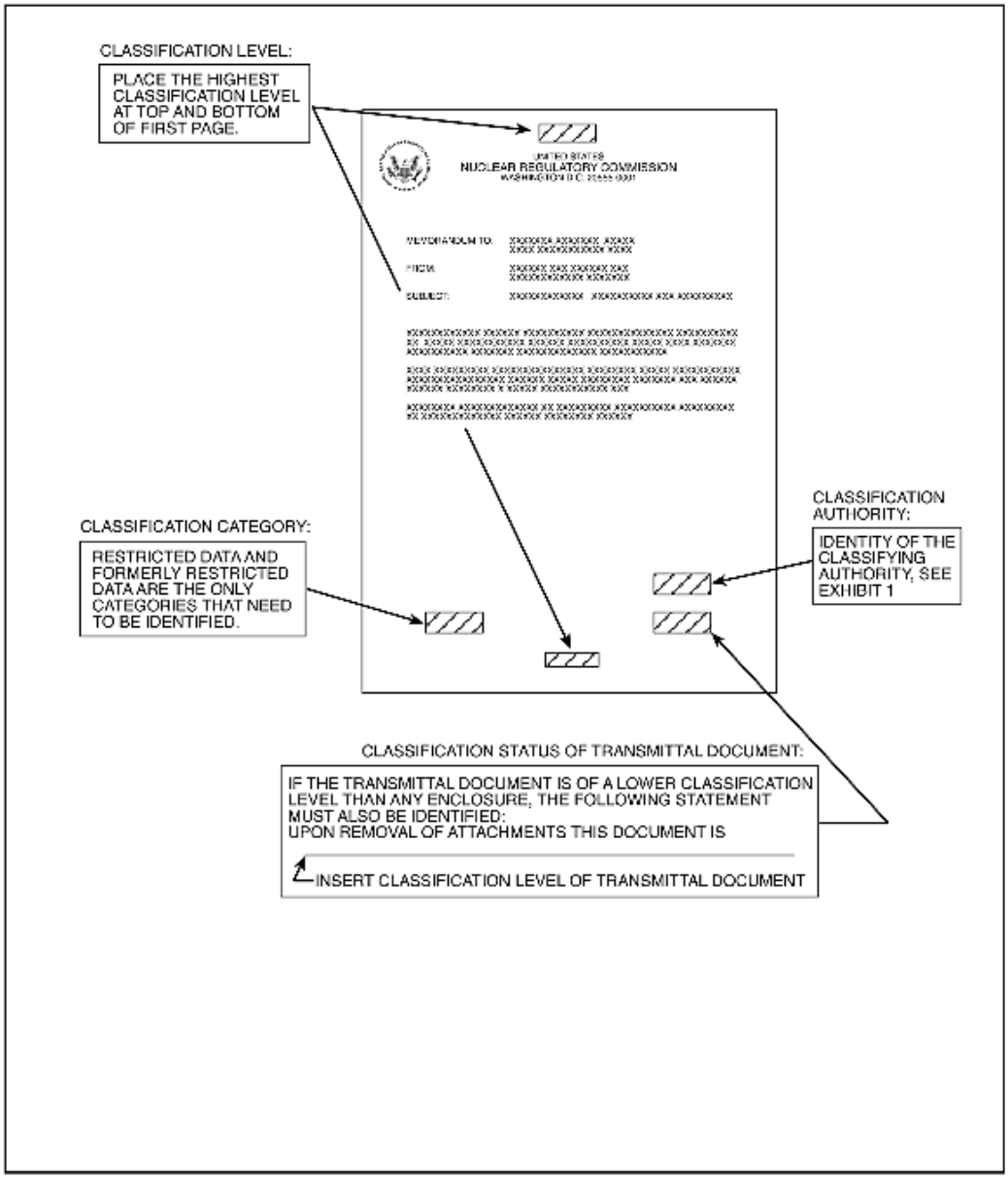
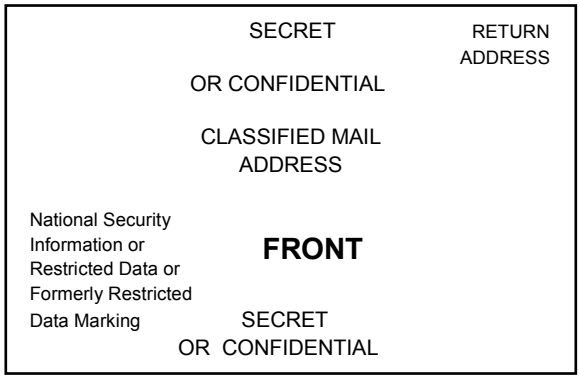
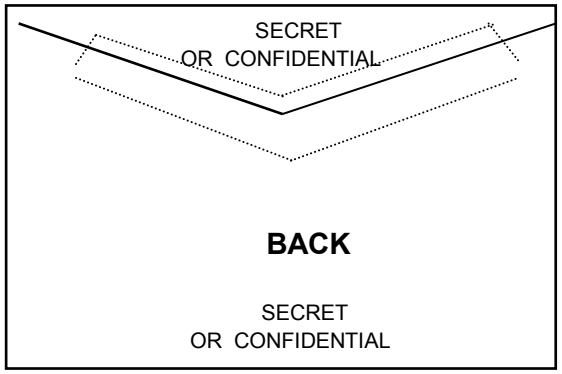


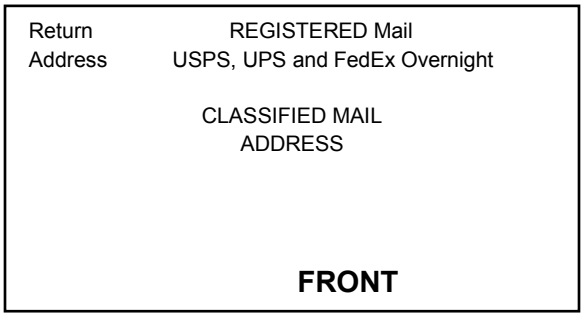
Exhibit 8 Required Markings for Envelopes or Wrappers

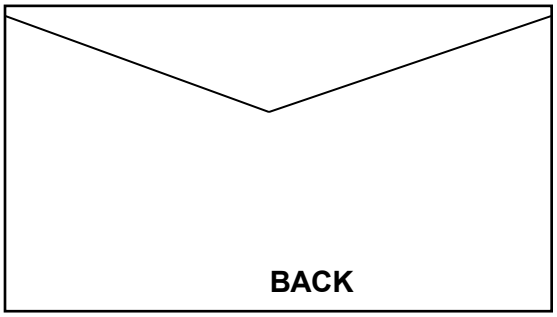
INNER ENVELOPE (OPAQUE)
SECRET OR CONFIDENTIAL



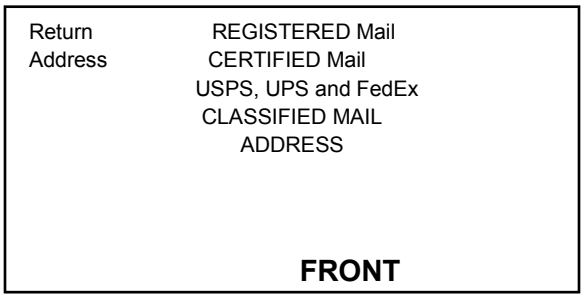


OUTER ENVELOPE (OPAQUE)
SECRET





OUTER ENVELOPE (OPAQUE)
CONFIDENTIAL



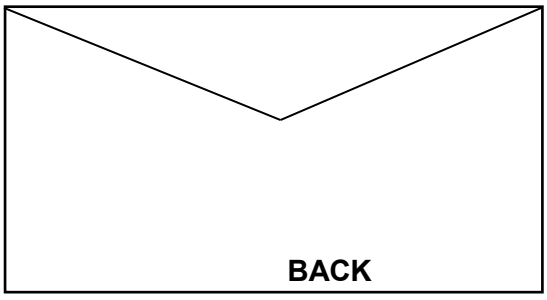


Exhibit 9 Foreign Equivalent Markings

Exhibit 9 is an excerpt from U.S. Department of Defense (DoD) Manual, "DoD Information Security Program: Marking of Classified Information," No. 5200.01, Vol. 2, dated February 24, 2013.

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Albania	TEPER SEKRET	SEKRET	IMIREBESUESHEM	I KUFIZUAR
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET or HIGHLY PROTECTED	CONFIDENTIAL or PROTECTED	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTS
Belgium (Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Bulgaria	СТРОГО СЕКРЕТНО (STROGO SECRETNO)	СЕКРЕТНО (SEKRETNO)	ПОВЕРИТЕЛНО (POVERITELNO)	ЗА СЛУЖЕБНО ПОЛЗВАНЕ (ZA SLUZHEBNO POLZVANE – equates to For Official Use)
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	RESERVADO	CONFIDENCIAL	
Colombia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENCIAL/ RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Croatia	NAJVECI TAJNITAJNI	TAJNI	POVERLJIV	OGRANCIEN
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO
Egypt	TOP SECRET	VERY SECRET	SECRET	OFFICIAL
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	
Estonia	TOP SECRET	SECRET	CONFIDENTIAL	
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN	Salainen	Luottamuksellinen	Viranomaiskaytto
France	TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	Vs- Nur für den Dienstgebrauch
Greece	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (AKROS APORRITO)	ΑΠΟΡΡΗΤΟ (APORRITO)	ΕΜΠΙΣΤΕΥΤΙΚΟ (EMPISTEUTIKO)	ΠΕΡΙΩΡΙΣΜΕΝΗΣΧΡΗΣΕΩΣ (PERIORISMENISCHER ISEOS)
Guatamala	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Hungary	SZIGORUAN TITKOS	TITKOS	TITKOS	KORLÁTOZOTT TERJESXTÉSŰ

Exhibit 9 (continued)

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Iceland	ALGJORTI	TRUNADARMAL	THJONUSTAJSKJAL	
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BENKOLI SERRI	SERRI	KHEILI MAHRAMANEH	MAHRAMANEH
Ireland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Israel	SODI BE'YOTER	SODI	SHAMUR	MUGBAL
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	TOP SECRET	SECRET	CONFIDENTIAL	
Jordan	STRICTLY CONFIDENTIAL	CONFIDENTIAL	RESTRICTED	
Korea	I KUP PI MIL	II KUP PI MIL	III KUP PI MIL	
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Latvia	SEVISKI SLEPENA	SLEPENA	KONFIDENCIALA	DIENESTA VAJADZĪBĂM
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Lithuania	VISIŠLAPTAI SLAPTAI	SLAPTAI	SLAPTAI	RIBOTO NAUDOJIMO
Malaysia	RAHSIA BESAR	RAHSIA	SULIT	TERHAD
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Morocco	SECRET DEFENSE	SECRET	CONFIDENTIEL	RESTREINT
Netherlands	STG. ZEER GEHEIM	STG. GEHEIM	STG. CONFIDENTIEEL	Departementaal VERTROUWELIJK
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENEIELT	BEGRENSET
Oman	TOP SECRET	SECRET	CONFIDENTIAL	
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	SCISLE TAJNE	TAJNE	POUFNE	ZASTREZONE
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romanian	STRICT-SECRET DE IMPORT ANT A DEOSEBITA	STRICT-SECRET	SECRET	SECRET DE SERVICIU

Exhibit 9 (continued)

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Saudi Arabia	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI RESTRICTED
Singapore	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Slovakia	PRÍSNE TAJNÉ	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	STROGO ZAUPNO	OBRAMBA – DRŽAVNA SKRIVNOST Defense - State Secret	ZAUPNO	
South Africa	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	H0/ TOP SECRET (the word HEMLIG enclosed with Red Borders)	H1/ SECRET	H2/ SECRET	
Switzerland	GEHEIM	VERTAULICH		
Taiwan	TOP SECRET (Not translatable into English characters)	SECRET	CONFIDENTIAL	
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Tunisia	TOP SECRET	SECRET	SECRET CONFIDENTIAL	
Turkey	COK GIZLI	GIZLI	OZEL	HIZMETE ÖZEL
Ukraine	ОСОБЛИВОЇ ВАЖЛИВОСТІ (OSOBLIVOI VAZHLIVOSTI)	ЦІЛКОМ ТАЄМНО (SHCHLKOM TAEMNO)	ТАЄМНО (TAEMNO)	
UK	TOP SECRET	SECRET		OFFICIAL
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO