



## Department of Energy

Washington, DC 20585

APR 18 2005

Ms. Anna Bradford  
Senior Project Manager  
Division of Waste Management  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852

Dear Ms. Bradford:

The purpose of this letter is to describe the public release review that was conducted on the Department of Energy (DOE) draft Section 3116 Determination for Salt Waste Disposal at the Savannah River Site (SRS) and the reference documents. The following information is provided in response to your email of March 15, 2005.

The SRS information/document release process consists of the following DOE programs and reviews:

- Operations Security (OPSEC)
- Classification/Unclassified Controlled Nuclear Information (UCNI)/Official Use Only (OUO)
- Export Control
- Scientific and Technical Information (STI) Management
- SRS Office of Chief Counsel
- SRS Office of External Affairs

The OPSEC review identifies sensitive SRS operational information which could be used to target DOE facilities, operations, and personnel. The DOE issued guidance on the control of sensitive operational information in October 2001 based on similar guidelines from the Assistant to the President and Chief of Staff and the U.S. Attorney General in the aftermath of the September 11, 2001, terrorist attacks on the United States. The review is similar to the sensitive operations information reviews conducted on the U.S. Nuclear Regulatory Commission (NRC) nuclear power reactor licensees. This review ensures that sensitive operations or facility information, which could assist an adversary in planning or executing a malevolent act, is not released to the public.



The Classification/UCNI/OUO programs review identifies restricted data, formerly restricted data, national security information, information related to the design of nuclear material production/utilization facilities, security information, and Freedom of Information Act-exempt information through a system of DOE approved classification and UCNI/OUO guides. This review ensures that classified or sensitive unclassified information is not inadvertently released to the public. Our understanding is that the NRC would follow similar processes in reviewing documents originated by the agency. For more details, see the following references: 10 CFR Part 1045, 10 CFR Part 1017, and 10 CFR Part 1004, which are the bases for DOE's processes.

The Export Control program reviews documents for technical data controlled by 15 CFR 730-774 (Department of Commerce Export Administration Regulations), 10 CFR 810 (DOE Nuclear Fuel Cycle and Heavy Water Production Technology), and the U.S. Munitions List (Department of State 22 CFR 121). This review ensures that technical data, which could aid an adversary to proliferate the development or advancement of weapons of mass destruction programs or other technical data that could impact on U.S. National Policy objectives, is properly controlled.

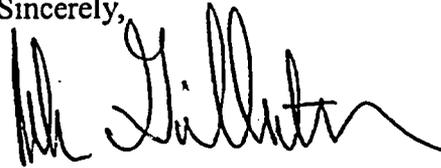
The STI review ensures that, in accordance with applicable laws and Departmental requirements, appropriate DOE funded STI is shared with the scientific community and the public through the DOE Office of Scientific and Technical Information. The Office of Chief Counsel ensures released information is reviewed for intellectual property, proprietary information, and provides a general legal review of the information. Finally, the Office of External Affairs ensures that information released is consistent with established DOE policies and procedures.

For your information, I am enclosing the following documents which describe these programs in more detail.

- DOE N 251.58, Extension of DOE Directives on Security
- DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information
- DOE M 471.1-1 (Change 1), Identification and Protection of Unclassified Controlled Nuclear Information Manual
- DOE Order 471.2A, Information Security Program
- DOE O 471.3, Identifying and Protecting Official Use Only Information
- DOE M 471.3-1, Manual for Identifying Official Use Only Information
- DOE M 475.1-1A, Identifying Classified Information
- DOE Guidelines on Export Control and Nonproliferation

I hope this information is helpful. If we can be of further assistance, please call Mr. Kenneth Picha at (202) 586-9726.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark A. Gilbertson". The signature is fluid and cursive, with a long horizontal flourish at the end.

Mark A. Gilbertson  
Deputy Assistant Secretary for  
Environmental Cleanup and Acceleration  
Office of Environmental Management

8 Enclosures

United States Department of Energy

**Directives, Regulations,  
and Standards**Managed by the  
Office of Management  
Communications, ME-43**Directives Regulations Standards References DOE Forms Delegations**[Home](#) [Comments](#) [Help](#) [Search](#) [Up](#) [Previous Record](#) [Next Record](#)The PDF version 

Display Related Directives to this directive.

Display Reference Documents to this directive.

U.S. Department of Energy  
Washington, D.C.

NOTICE

DOE N 251.58

Approved: 7-6-04

Expires: 6-30-05

SUBJECT: EXTENSION OF DOE DIRECTIVES ON SECURITY

The following Directives are extended until 6-30-05.

DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information,  
dated 6-30-00.DOE M 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information  
Manual, dated 6-30-00.The two unclassified controlled nuclear information (UCNI) Directives will be revised when the  
UCNI regulation (10 CFR Part 1017) completes the revision process.

DOE O 473.2, Protective Force Program, dated 6-30-00.

The requirements of DOE O 473.2 will be incorporated into a Manual at a later date.

If you have any questions concerning this action, please contact Geralyn Praskievicz at  
202-586-4451.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW  
Deputy Secretary.AVAILABLE ONLINE AT:  
<http://www.directives.doe.gov>INITIATED BY:  
Office of Security[Home](#) [Comments](#) [Help](#) [Search](#) [Up](#) [Previous Record](#) [Next Record](#)

**U.S. Department of Energy**  
Washington, D.C.

**ORDER**

DOE O 471.1A

Approved: 6-30-00  
Sunset Review: 6-30-02  
Expires: 6-30-04

**SUBJECT: IDENTIFICATION AND PROTECTION OF UNCLASSIFIED  
CONTROLLED NUCLEAR INFORMATION**

---

1. **OBJECTIVE.** To prevent the unauthorized dissemination of Unclassified Controlled Nuclear Information (UCNI).
2. **CANCELLATION.** DOE O 471.1, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, dated 9-25-95.
3. **APPLICABILITY.**
  - a. **DOE Elements.** This Order applies to all DOE elements, including the National Nuclear Security Administration (NNSA), that may generate, possess, or have access to information or matter containing UCNI.
  - b. **Contractors.** The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements to be applied to DOE, including NNSA, contractors that may generate, possess, or have access to information or matter containing UCNI. Contractor compliance with the CRD is required to the extent set forth in a contract.
4. **REQUIREMENTS.** Detailed requirements for identifying and protecting UCNI are contained in DOE M 471.1-1, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION MANUAL.
  - a. Any person who originates or possesses unclassified matter that may contain UCNI must send the unclassified matter to a Reviewing Official.
  - b. A Reviewing Official (see DOE M 471.1-1, Chapter I, Part B) determines whether matter contains UCNI and marks or authorizes it to be marked as required in DOE M 471.1-1, Chapter I, Part C.
  - c. A Denying Official (see DOE M 471.1-1, Chapter I, Part B) determines whether matter requested under statute or Executive order is exempt from release based on a Reviewing Official's recommendation and applicable UCNI guidelines.

---

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Office of Security Affairs

- d. Access to UCNI must be provided to only those individuals authorized for routine or special access (see DOE M 471.1-1, Chapter II).
- e. Physical protection requirements for UCNI are contained in DOE M 471.1-1, Chapter II.

5. RESPONSIBILITIES.

- a. Director of Security Affairs.
  - (1) Oversees the program to identify and protect UCNI.
  - (2) Determines whether a material is a "nuclear material" under 10 Code of Federal Regulations (CFR) 1017.10.
  - (3) Determines whether any portion of a document requested under statute or Executive order that was initially denied because it contained UCNI still contains UCNI and must still be denied.
- b. Director of Nuclear and National Security Information.
  - (1) Administers the program to identify UCNI (see DOE M 471.1-1, Chapter I).
  - (2) Determines whether specific Government information is UCNI as the Controlling Official under 10 CFR 1017.7.
  - (3) Develops and issues the UCNI General Guideline and all Topical Guidelines; approves all UCNI guidelines.
  - (4) Trains and designates Reviewing Officials for Headquarters elements and their contractors and for any organization or contractor with no Classification Officer.
  - (5) Trains and designates Reviewing Officials who may review matter for UCNI that is not under their own programmatic or organizational cognizance.
  - (6) Resolves disagreements between Reviewing and/or Denying Officials about whether matter contains UCNI.
  - (7) Issues, and makes available upon request to any interested person, a quarterly report describing and justifying Government information determined to be UCNI during the previous quarter.

- (8) Manages the UCNI oversight program to ensure that DOE and NNSA elements and their contractors that generate information or matter containing UCNI effectively carry out those requirements in DOE M 471.1-1 concerning the identification of UCNI.
- c. Director of Safeguards and Security. Administers the program to protect UCNI (except for information being processed, stored, or transmitted in unclassified automated information systems). See DOE M 471.1-1, Chapters II and III.
  - d. Chief Information Officer. Administers the program to protect UCNI being processed, stored, or transmitted in unclassified automated information systems.
  - e. Heads of Program and Support Offices within DOE and NNSA and Managers of Field Elements.
    - (1) Ensure that the necessary staff are designated to fulfill the requirements contained in this Order.
    - (2) Identify/appoint an individual to determine which contracts (including M&O contracts, M&I contracts, non-M&O contracts, etc.) are subject to the requirements contained in the CRD attached to this Order and ensure that the CRD is incorporated in those contracts (when next modified or extended, but not later than 6 months from the date of this Order). If the requirements contained in the CRD are considered prohibitively expensive, then an existing contract may need to be terminated or renegotiated.
    - (3) Identify/appoint an individual to be responsible for notifying the contracting officer of each new procurement falling within the scope of the CRD attached to this Order. If such an individual is not identified or appointed, the person originating the procurement request assumes this responsibility.
  - f. Field Element Classification Officers (see DOE M 475.1-1, IDENTIFYING CLASSIFIED INFORMATION).
    - (1) Administer the UCNI identification program for their field elements.
    - (2) Are Reviewing Officials and may train and designate other Reviewing Officials from their organizations, subordinate organizations, and contractors under their cognizance.
    - (3) May overrule UCNI determinations made by Reviewing Officials under their cognizance.

- g. Deputy Administrator for Naval Reactors. Implements and oversees all policy and practices pertaining to this Order for activities under the Deputy Administrator's cognizance.
- h. Individuals Originating Procurement Requests (or such other individuals identified/appointed by the cognizant head of the DOE/NNSA element).
  - (1) Bring to the attention of the cognizant contracting officer the following:
    - (a) each procurement requiring the inclusion of all or part of the CRD attached to this Order and
    - (b) flowdown requirements to any subcontract or subaward.
  - (2) Identify the UCNI guidelines that apply to each proposed contract or subcontract action.
- i. Contracting Officers. Based on advice received from the person originating a procurement request or the individual identified/appointed by the head of the cognizant DOE/NNSA element, apply requirements contained in the CRD attached to this Order to DOE contractors.

## 6. REFERENCES.

- a. DOE M 471.1-1, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION MANUAL, dated 6-30-00.
- b. DOE M 475.1-1, IDENTIFYING CLASSIFIED INFORMATION, dated 5-8-98.
- c. 10 CFR PART 1017, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.

## 7. DEFINITIONS.

- a. Matter. Any combination of documents or material.
- b. Unclassified Controlled Nuclear Information. Certain unclassified but sensitive Government information concerning nuclear material, weapons, and components whose dissemination is controlled under section 148 of the Atomic Energy Act.

DOE O 471.1A  
6-30-00

5 (and 6)

8. CONTACT. Direct any questions regarding this Order to the Office of Nuclear and National Security Information, 301-903-5454, or to the Office of Safeguards and Security, 301-903-4805, as appropriate.

BY ORDER OF THE SECRETARY OF ENERGY:



T. J. GLAUTHIER  
DEPUTY SECRETARY

## ATTACHMENT 1

### CONTRACTOR REQUIREMENTS DOCUMENT

#### DOE O 471.1A, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, dated 6-30-00

In the performance of this contract, the contractor is responsible for complying with the following requirements and for flowing down all requirements to subcontractors:

1. If the contractor has a formally designated Classification Officer, the Classification Officer—
  - a. serves as a Reviewing Official for information under his/her cognizance;
  - b. trains and designates other Reviewing Officials in his/her organization, subordinate organizations, and subcontractors and maintains a current list of all Reviewing Officials; and
  - c. may overrule UCNI determinations made by Reviewing Officials under his/her cognizance.
2. If the contractor has no formally designated Classification Officer, the contractor submits a request for the designation of Reviewing Officials to the local Federal Classification Officer (for Headquarters, this is the Director of Nuclear and National Security Information) in accordance with the instructions contained in DOE M 471.1-1, Chapter I, Part B.
3. The contractor's Reviewing Officials use appropriate UCNI guidelines (i.e., General Guideline, Topical Guidelines, Internal Guidelines; see DOE M 471.1-1, Chapter I, Part A) to review matter and identify what specific Government information is UCNI, in accordance with the instructions contained in DOE M 471.1-1, Chapter I, Part B.
4. The contractor develops and issues UCNI internal guidelines, as necessary and with the approval of the local Federal Classification Officer, if appropriate, and the Director of Nuclear and National Security Information, in accordance with the instructions contained in DOE M 471.1-1, Chapter I, Part A.
5. The contractor's Reviewing Officials apply or authorize the application of UCNI markings to any unclassified matter that contains UCNI in accordance with the instructions contained in DOE M 471.1-1, Chapter I, Part C.

6. The contractor ensures that access to UCNI is provided to only those individuals authorized for routine or special access (see DOE M 471.1-1, Chapter II).
7. The contractor ensures that matter identified as UCNI is protected in accordance with the instructions contained in DOE M 471.1-1, Chapter II.
8. The contractor reports to the facility security office any incidents involving the unauthorized disclosure of UCNI.

DOE M 471.1-1

Approved: 6-30-00  
Sunset Review: 6-30-02  
Expiration: 6-30-04  
Change 1: 10-23-01

# IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION MANUAL

---



**U.S. DEPARTMENT OF ENERGY**  
Office of Security and Emergency Operations  
Office of Security Affairs  
Office of Nuclear and National Security Information  
Office of Safeguards and Security

---

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Office of Security Affairs

**IDENTIFICATION AND PROTECTION OF  
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION MANUAL**

---

1. **PURPOSE.** This Manual provides detailed requirements to supplement DOE O 471.1A, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION.
2. **SUMMARY.** This Manual is composed of three chapters that provide the requirements for identifying and protecting Unclassified Controlled Nuclear Information (UCNI). Chapter I describes how UCNI is identified in matter, including the authority needed to review matter, the guidelines that are used, and the markings that are placed on the matter. Chapter II describes the access and physical protection requirements. Chapter III describes how violations and infractions of requirements in this Manual are handled.
3. **REFERENCES.**
  - a. DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, dated 9-28-95.
  - b. DOE O 471.1A, IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, dated 6-30-00.
  - c. DOE M 475.1-1, IDENTIFYING CLASSIFIED INFORMATION, dated 5-8-98.
  - d. DOE 3750.1, WORK FORCE DISCIPLINE, dated 3-23-83.
  - e. 10 CFR Part 1004, "Freedom of Information."
  - f. 10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information."
  - g. Atomic Energy Act of 1954, as amended, section 123, "Cooperation with Other Nations" (42 U.S.C. 2153); and section 148, "Dissemination of Unclassified Information" (42 U.S.C. 2168).
4. **DEVIATIONS FROM REQUIREMENTS.**
  - a. **Deviations from Chapter I Requirements.** A Classification Officer may propose an alternate or equivalent means of meeting a specific requirement in Chapter I or he/she may request an exemption. Such a proposal shall describe the variance or waiver and explain why it is needed. The proposal must be submitted to the Director of Nuclear and National Security Information for approval. The

Director's decision must be made within 30 days. Each approved deviation will be examined during an oversight review to ensure it is still needed.

- b. Deviations from Chapter II or III Requirements. Deviations from requirements contained in Chapter II or III will be approved through procedures established in DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.
4. CONTACT. Questions concerning this Manual should be addressed as follows:
    - a. Questions on Chapter I should be directed to the Office of Nuclear and National Security Information at 301-903-5454.
    - b. Questions on Chapters II and III should be directed to the Office of Safeguards and Security at 301-903-4805.

BY ORDER OF THE SECRETARY OF ENERGY:



T. J. GLAUTHIER  
DEPUTY SECRETARY

CONTENTS

CHAPTER I: IDENTIFICATION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Part A—Guidelines ..... I-1

1. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION GUIDELINES ..... I-1

2. GENERAL GUIDELINE ..... I-1

    a. Purpose ..... I-1

    b. Originator/Approval Authority ..... I-1

    c. Basis ..... I-1

    d. Uses ..... I-1

        (1) Review of Matter ..... I-1

        (2) Denial of Matter ..... I-1

    e. Identification Number ..... I-1

3. TOPICAL GUIDELINES ..... I-2

    a. Purpose ..... I-2

    b. Originator/Approval Authority ..... I-2

    c. Basis ..... I-2

    d. Uses ..... I-2

        (1) Review of Matter ..... I-2

        (2) Denial of Matter ..... I-2

    e. Basis Citation ..... I-2

4. INTERNAL GUIDELINES ..... I-2

    a. Purpose ..... I-2

    b. Originator/Approval Authority ..... I-2

    c. Basis ..... I-3

    d. Uses ..... I-3

        (1) Review of Matter ..... I-3

        (2) Denial of Matter ..... I-3

    e. Basis Citation ..... I-3

    f. Submission of Guideline for Approval ..... I-3

    g. Copies of the Guideline ..... I-3

Part B—Review of Matter ..... I-4

1. OVERVIEW ..... I-4

## CONTENTS (continued)

2.	REVIEWING OFFICIALS .....	I-4
a.	Authority .....	I-4
b.	Designation of Reviewing Officials .....	I-4
	(1) Field .....	I-4
	(2) Headquarters .....	I-4
c.	List of Current Reviewing Officials .....	I-5
d.	Cancellation of Authority .....	I-5
	(1) By the Reviewing Official's Office Director .....	I-5
	(2) By the Designating Official .....	I-5
	(3) By the Field Element Classification Officer .....	I-5
	(4) By the Chief of Defense Nuclear Security .....	I-5
	(5) By the Director of Nuclear and National Security Information .....	I-6
3.	REVIEW RESPONSIBILITIES .....	I-6
a.	Responsibilities of Originator or Possessor of Matter .....	I-6
	(1) Review Requirement .....	I-6
	(2) Review Requirement Exception .....	I-6
b.	Responsibilities of the Reviewing Official .....	I-6
	(1) When Applicable Topical or Internal Guidelines Exist .....	I-6
	(2) When No Applicable Topical or Internal Guidelines Exist .....	I-6
c.	Review Responsibilities of Classification Officers .....	I-7
	(1) When Applicable General Guideline Topics Exist .....	I-7
	(2) When No Applicable General Guideline Topics Exist .....	I-7
d.	Notification of Determination .....	I-7
e.	Scientific and Technical Reports .....	I-7
4.	DENIAL OF MATTER CONTAINING UCNI REQUESTED REQUESTED UNDER STATUTE OR EXECUTIVE ORDER .....	I-7
a.	Denial Determination .....	I-7
b.	Denial Notification Requirements .....	I-8
	(5) Originator .....	I-8
	(6) Office of Nuclear and National Security Information .....	I-8
	(7) Office of Scientific and Technical Information .....	I-8
5.	APPEAL OF THE DENIAL OF MATTER BY A DENYING OFFICIAL .....	I-8
a.	Authority .....	I-8
b.	Analytical Support .....	I-8
c.	Scientific and Technical Reports .....	I-8
6.	JOINT MATTER .....	I-9
7.	MATTER SENT TO FILES .....	I-9

CONTENTS (continued)

Part C—Marking of Matter ..... I-10

1. RELATIONSHIP TO OTHER TYPES OF CONTROL MARKINGS ..... I-10

    a. Unclassified Matter ..... I-10

    b. Classified Matter ..... I-10

2. UNCLASSIFIED MATTER THAT CONTAINS UCNI ..... I-10

    a. Front Marking ..... I-10

    b. Page Marking ..... I-10

    c. Removal of Markings ..... I-10

3. USE OF ALTERNATE MARKINGS ..... I-11

    a. Conditions of Use ..... I-11

    b. Alternate Markings ..... I-11

4. CAVEAT ..... I-11

5. SPECIAL FORMAT MATTER ..... I-12

6. TRANSMITTAL DOCUMENTS ..... I-12

7. UNCLASSIFIED MATTER THAT NO LONGER CONTAINS UCNI ..... I-12

8. UNCLASSIFIED MATTER THAT DOES NOT CONTAIN UCNI ..... I-12

9. UPGRADING ..... I-13

CHAPTER II: PROTECTION OF UCNI

1. ACCESS TO UCNI ..... II-1

    a. Routine Access ..... II-1

        (1) Authorized Individual ..... II-1

        (2) Eligibility for Routine Access ..... II-1

            (a) U.S. Citizen ..... II-1

            (b) Other Than a U.S. Citizen ..... II-2

            (c) Other Than a U.S. Citizen and Otherwise Not Eligible  
                for Routine Access ..... II-2

        (3) Dissemination Limitations ..... II-3

        (4) Access to UCNI Matter by Prospective Contractors in Bid Rooms ..... II-3

        (5) Deviation from Requirements ..... II-3

    b. Special Access ..... II-3

        (1) Submission of a Request ..... II-3

**CONTENTS (continued)**

- (2) Granting a Request ..... II-3
- (3) Notification to the Office of Safeguards and Security ..... II-4
- (4) Notification of Requester ..... II-4
- (5) Special Access Limitations ..... II-4
- (6) Categorical Special Access Approval ..... II-4
- (7) Notification of Responsibilities by Use of Cover Sheet ..... II-4
  
- 2. PHYSICAL PROTECTION REQUIREMENTS ..... II-5
  - a. Protection in Use ..... II-5
  - b. Protection in Storage ..... II-5
  - c. Reproduction ..... II-5
  - d. Destruction ..... II-5
  - e. Transmission ..... II-6
    - (1) Outside a Facility ..... II-6
    - (2) Within a Facility ..... II-6
    - (3) Over Telecommunications Circuits ..... II-6
  - f. Automated Information Systems (AIS) ..... II-6

**CHAPTER III: VIOLATIONS AND INFRACTIONS**

- 1. VIOLATIONS ..... III-1
- 2. INFRACTIONS ..... III-1

## CHAPTER I

### IDENTIFICATION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

#### Part A - Guidelines

1. UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI) GUIDELINES.  
Reviewing and Denying Officials must use UCNI guidelines as their basis for determining whether matter contains UCNI. Such guidelines may be separate documents or integrated in classification guides. These guidelines are of three types: the General Guideline, Topical Guidelines, and Internal Guidelines.
2. GENERAL GUIDELINE.
  - a. Purpose. The General Guideline contains general policies and identifies whether broad areas of information are UCNI. In addition, the General Guideline is the basis for Topical and Internal Guidelines.
  - b. Originator/Approval Authority. The General Guideline is approved and issued by the Office of Nuclear and National Security Information.
  - c. Basis. The General Guideline is based on determinations by the Director of Nuclear and National Security Information.
  - d. Uses.
    - (1) Review of Matter. A Reviewing Official in the Office of Nuclear and National Security Information or a DOE field element or contractor Classification Officer may use the General Guideline to determine whether information is UCNI in any subject area for which Topical or Internal Guidelines do not exist.
    - (2) Denial of Matter. A Denying Official may use the General Guideline to determine whether information is UCNI in any subject area for which Topical or Internal Guidelines do not exist.
  - e. Identification Number. Each topic in the General Guideline which states that information is UCNI must include a unique and permanent identification number (e.g., GG #10).

### 3. TOPICAL GUIDELINES.

- a. Purpose. A Topical Guideline identifies whether information in a specific technical or program area is UCNI.
- b. Originator/Approval Authority. The Office of Nuclear and National Security Information approves and issues Topical Guidelines.
- c. Basis. A Topical Guideline is based on the General Guideline or another Topical Guideline.
- d. Uses.
  - (1) Review of Matter. Any Reviewing Official may use a Topical Guideline to determine whether information is UCNI.
  - (2) Denial of Matter. A Denying Official may use a Topical Guideline to determine whether information is UCNI.
- e. Basis Citation. Each topic in a Topical Guideline that designates information as UCNI must cite the identification number of either the General or Topical Guideline on which it is based. In addition, each topic in a Topical Guideline that indicates information is UCNI must include a Topical Guideline identification number (e.g., NV-TG #1) to be cited as the basis for either Topical or Internal Guideline topics.

### 4. INTERNAL GUIDELINES.

- a. Purpose. An Internal Guideline identifies whether information of interest to the issuing organization is UCNI.
- b. Originator/Approval Authority. DOE elements, including National Nuclear Security Administration (NNSA), and contractor organizations may issue Internal Guidelines.
  - (1) The Office of Nuclear and National Security Information must approve each Internal Guideline before it is issued or reissued. The Director of Nuclear and National Security Information may delegate this authority in writing to field element Classification Officers.
  - (2) Internal Guidelines are not required to be issued by any organization if Topical Guidelines and the General Guideline are adequate for the needs of the organization.

- c. Basis. An Internal Guideline is based on a Topical Guideline; however, if no applicable Topical Guideline exists, the Internal Guideline may be based directly on the General Guideline.
- d. Uses. The issuing organization should specify in the Internal Guideline which organizations are authorized to use the Internal Guideline to determine whether information is UCNI.
  - (1) Review of Matter. Only Reviewing Officials in the Office of Nuclear and National Security Information, Reviewing Officials within the issuing organization, and those Reviewing Officials who have been authorized within the Internal Guideline or otherwise in writing by the issuing organization may use an Internal Guideline to determine whether information is UCNI.
  - (2) Denial of Matter. Any Denying Official may use an Internal Guideline generated by an organization under his/her cognizance to determine that information is UCNI.
- e. Basis Citation. Each topic in an Internal Guideline that states that information is UCNI must cite the General Guideline or Topical Guideline identification number on which the topic is directly based.
- f. Submission of Guideline for Approval. An organization that submits an Internal Guideline to the Office of Nuclear and National Security Information for review and approval must include the following:
  - (1) the full text of the guideline;
  - (2) a justification for any deviations to current policy proposed in the draft guideline;
  - (3) a contact point for requesting approval for use of the guideline by Reviewing or Denying Officials not authorized to use the Internal Guideline; and
  - (4) a contact point for requesting copies of the guideline.
- g. Copies of the Guideline. Any organization that issues an Internal Guideline must send the Office of Nuclear and National Security Information one floppy diskette in either ASCII or WordPerfect 5.1 or higher format and five copies of the issued guideline.

**Part B - Review of Matter**

1. **OVERVIEW.** Any matter that may contain UCNI must be sent to a Reviewing Official prior to release. A Reviewing Official determines whether the matter contains UCNI. A Reviewing Official bases his/her determination on Topical Guidelines and Internal Guidelines. If matter containing UCNI is requested under a statute or Executive order, the Reviewing Official must send the matter to a Denying Official.
2. **REVIEWING OFFICIALS.**
  - a. **Authority.** A Reviewing Official with cognizance over information contained in matter (or as designated by the Office of Nuclear and National Security Information) must determine whether the matter contains UCNI. A Reviewing Official authorizes UCNI markings to be applied to or removed from matter. The Reviewing Official's authority may not be redelegated to anyone or exercised by a person acting for or in the absence of the Reviewing Official.
  - b. **Designation of Reviewing Officials.**
    - (1) **Field.** DOE field element and contractor Classification Officers train and designate additional Reviewing Officials as necessary within their organizations, subordinate organizations, and contractors. Any individual in a position that requires Reviewing Official authority must submit a request to the local Classification Officer following local procedures.
    - (2) **Headquarters.** The Office of Nuclear and National Security Information trains and designates Reviewing Officials for Headquarters and NNSA elements and their contractors and for any organization or contractor with no Classification Officer. Any individual in a position that requires Reviewing Official authority must submit a request signed by the office director or higher-level official to the Office of Nuclear and National Security Information. This request must contain the following information:
      - (a) name of the individual requiring the authority;
      - (b) title, mailing address (including organization code), and telephone number of the individual;
      - (c) whether the individual is a Federal employee or a contractor;
      - (d) why the authority is required;

- (e) anticipated frequency of use of the authority (e.g., daily, weekly);
  - (f) UCNI guideline(s) to be used (a list of guidelines is available from the Office of Nuclear and National Security Information); and
  - (g) qualifications of the individual (include educational background and experience).
- c. List of Current Reviewing Officials. Each designating official must maintain a current list of all Reviewing Officials under his/her cognizance. This list must include the following information:
- (1) name, title, and organization of each Reviewing Official;
  - (2) effective date of each designation; and
  - (3) any special instructions or limitations that apply to each designation.
- d. Cancellation of Authority. The Reviewing Official's office director, the designating official, the field element Classification Officer for contractors under his/her cognizance, the Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel Reviewing Official authority when the employee's position no longer requires such authority or the employee cannot or does not exercise that authority reliably.
- (1) By the Reviewing Official's Office Director. The office director who cancels the Reviewing Official authority for an employee must notify the employee and inform the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
  - (2) By the Designating Official. The designating official who cancels the Reviewing Official authority for an employee must notify the employee and inform the employee's office director of the employee's name and position, the reason for cancellation, and the date the authority will end.
  - (3) By the Field Element Classification Officer. The field element Classification Officer who cancels the Reviewing Official authority for a contractor employee under his/her cognizance must notify the employee and inform the employee's office director and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.

4. By the Chief of Defense Nuclear Security. Upon canceling the Reviewing Official authority for an employee within NNSA, the Chief of Defense Nuclear Security must notify the employee and inform the employee's office director and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (5) By the Director of Nuclear and National Security Information. Upon canceling the Reviewing Official authority for an employee, the Director of Nuclear and National Security Information must notify the employee and inform the employee's office director and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.

### 3. REVIEW RESPONSIBILITIES.

- a. Responsibilities of Originator or Possessor of Matter.
  - (1) Review Requirement. Any person who thinks unclassified matter he/she originates or possesses may contain UCNI must send it to a Reviewing Official before it is finalized, sent outside of the organization, or filed. (NOTE: Matter retrieved from the files for reference, inventory, or similar purposes does not have to be reviewed for UCNI, as long as it will be returned to the files and is not accessible by individuals who are not authorized access to UCNI.)
  - (2) Review Requirement Exception. Review is not required of matter sent outside the originator's or possessor's organization for destruction. However, any matter being destroyed that is not marked as containing UCNI but that the originator or possessor believes may contain UCNI must be destroyed in accordance with procedures in Chapter II, paragraph 2d.
- b. Responsibilities of the Reviewing Official. A Reviewing Official must first determine whether the matter is widely disseminated in the public domain (e.g., a document that is available in a public or university library or over the Internet); such matter is exempt from control as UCNI regardless of its content. If not widely disseminated, the Reviewing Official determines whether the matter contains UCNI.
  - (1) When Applicable Topical or Internal Guidelines Exist. A Reviewing Official uses applicable Topical or Internal Guidelines authorized for his/her use to determine whether matter contains UCNI. The Reviewing Official applies or authorizes UCNI markings to be applied to the matter and notifies the originator.

- (2) When No Applicable Topical or Internal Guidelines Exist. When no applicable Topical or Internal Guidelines exist, the Reviewing Official must send the matter and written recommendations on information that should be designated as UCNI to the local Classification Officer, or for Headquarters, to the Office of Nuclear and National Security Information.

c. Review Responsibilities of Classification Officers.

- (1) When Applicable General Guideline Topics Exist. A Classification Officer may determine whether matter contains UCNI based on applicable General Guideline topics. The Classification Officer applies or authorizes UCNI markings to be applied to the matter and notifies the Reviewing Official who referred the matter. A Classification Officer may delegate this authority to Reviewing Officials on his/her immediate staff; otherwise, this authority must not be delegated.

- (2) When No Applicable General Guideline Topics Exist. When no applicable General Guideline topics exist, the Classification Officer must send the matter and written recommendations on information that should be designated as UCNI to the Office of Nuclear and National Security Information for a determination.

- d. Notification of Determination. A Reviewing Official must notify the originator of any unclassified matter determined to contain or no longer contain UCNI. To the extent practical, the originator should notify all holders of the matter of the determination.

- e. Scientific and Technical Reports. The originator must report to the Office of Scientific and Technical Information the title, number, date, originating organization, author, and UCNI status of any unclassified scientific and technical report that he/she determines contains UCNI.

4. DENIAL OF MATTER CONTAINING UCNI REQUESTED UNDER STATUTE OR EXECUTIVE ORDER.

- a. Denial Determination. UCNI is exempt from public release. Therefore, whenever any matter determined to contain UCNI by a Reviewing Official is requested under statute or Executive order, a Denying Official may deny the request for those portions. This is true regardless of whether the matter previously had UCNI markings. Denying Officials for Headquarters and field elements are defined in 10 CFR 1004.2(b) and deny unclassified matter requested under any statute or Executive order. The Reviewing Official processing the request must bracket each portion of the matter that the Reviewing Official believes contains UCNI prior to sending the matter to the

appropriate Denying Official. The Denying Official must then review the requested matter and ensure that the Reviewing Official has correctly interpreted and applied the UCNI guidelines. The Denying Official's determination is based on the Reviewing Official's recommendation and applicable UCNI guidelines.

b. Denial Notification Requirements.

- (1) Originator. To the extent practical, the Denying Official should notify the originator of any matter that was previously marked to indicate it may contain or does contain UCNI whenever the matter is released by the Denying Official because he/she has determined it no longer contains UCNI. To the extent practical, the originator should notify all holders of the matter of the determination.
- (2) Office of Nuclear and National Security Information. The Denying Official must notify the Office of Nuclear and National Security Information (ATTN: SO-221) of each denial determination and must provide that office with a copy of the request letter, the denial letter, and any analysis supporting the denial determination. (The Denying Official does not have to provide copies of the matter that was the subject of the request unless specifically requested by the Office of Nuclear and National Security Information.)
- (3) Office of Scientific and Technical Information. A Denying Official must notify the Office of Scientific and Technical Information of the title, number, date, originating organization, and author when an unclassified scientific or technical report previously marked to indicate it may contain or does contain UCNI is determined by the Denying Official to no longer contain UCNI.

5. APPEAL OF THE DENIAL OF MATTER BY A DENYING OFFICIAL.

- a. Authority. The Director of Security Affairs makes the determination regarding the denial of UCNI for all appeals involving requests for matter made under statute or Executive order. The Director of Hearings and Appeals issues the final appeal determination on behalf of DOE for requests made under statute; the Director of Security Affairs issues the final appeal determination for requests made under Executive order.
- b. Analytical Support. The Office of Nuclear and National Security Information provides analytical support and recommendations to assist the Director of Security Affairs in exercising his/her UCNI appeal authority.

- c. Scientific and Technical Reports. The Office of Nuclear and National Security Information must report to the Office of Scientific and Technical Information and the originator the title, number, date, originating organization, and author of any unclassified scientific or technical report that is determined on appeal to no longer contain UCNI.
6. JOINT MATTER. Prior to determining that matter under the cognizance of another DOE element no longer contains UCNI, the Reviewing Official must either send the matter to that organization for review or obtain the concurrence of that organization that the matter no longer contains UCNI.
7. MATTER SENT TO FILES. Any matter that has been filed is not required to be reviewed for UCNI while in the files or when retrieved from the files for reference, inventory, or similar purposes as long as it will be returned to the files and is not accessible by individuals who are not authorized access to UCNI. Such matter may or may not have any UCNI markings. However, any such unclassified matter that is proposed for release that is likely to contain UCNI must be reviewed by a Reviewing Official with cognizance over the information. Such circumstances requiring this proposed release might be a formal request for the matter under a statute or Executive order, response to a court order, or simply to answer a question from a DOE customer. If the matter is determined to contain UCNI, it must be marked by the document custodian in accordance with this chapter upon notification that the matter contains UCNI.

**Part C - Marking of Matter**

1. RELATIONSHIP TO OTHER TYPES OF CONTROL MARKINGS.

- a. Unclassified Matter. UCNI markings must be applied to any unclassified matter that contains or reveals UCNI regardless of any other unclassified control marking (e.g., Official Use Only, company "proprietary") that is also on the matter.
- b. Classified Matter. UCNI markings must not be applied to classified matter that contains UCNI, unless such matter has been portion marked to indicate the classification level. In such cases, the acronym "UCNI" must be used to indicate those unclassified portions containing UCNI.

2. UNCLASSIFIED MATTER THAT CONTAINS UCNI.

- a. Front Marking. When a Reviewing Official determines that unclassified matter contains UCNI, the Reviewing Official marks or authorizes the front of the matter to be marked as follows:

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION  
NOT FOR PUBLIC DISSEMINATION

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Reviewing  
Official: \_\_\_\_\_  
(Name/Organization)

Date: \_\_\_\_\_

Guidance Used: \_\_\_\_\_  
(List all UCNI guidance used)

- b. Page Marking. The marking "UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UCNI" must be placed on the top and bottom of the front of the matter and (1) on the top and bottom of each interior page of the matter or (2) if more convenient, on the top and bottom of only those interior pages that contain UCNI.

- c. Removal of Markings. The removal of these markings may be authorized by (1) the Reviewing Official who applied them; (2) the local Classification Officer or his/her delegate or, for Headquarters, the Office of Nuclear and National Security Information; or (3) a Denying Official.

### 3. USE OF ALTERNATE MARKINGS.

- a. Conditions of Use. Alternate markings may be applied to unclassified matter determined by a Reviewing Official to contain UCNI only if both of the following conditions are true:
  - (1) The matter is related to an atomic energy defense program, but does not contain any information explicitly indicating this relationship.
  - (2) The fact of the relationship of the matter to an atomic energy defense program is itself sensitive.
- b. Alternate Markings. The following markings may be used only if a Reviewing Official determines that the conditions of use described above are satisfied. All other standard markings specified in this chapter must be used as appropriate.
  - (1) Alternate Determination Marking. The Reviewing Official marks or authorizes the front of the matter to be marked as follows:

NOT FOR PUBLIC DISSEMINATION

Unauthorized dissemination subject to civil  
and criminal sanctions under 42 U.S.C. 2168.

- (2) Alternate Page Marking. The marking "UNCLASSIFIED CONTROLLED INFORMATION" must be placed on the top and bottom of the front of the matter and (1) on the top and bottom of each interior page of the matter or (2) if more convenient, on the top and bottom of only those interior pages that contain UCI.
4. CAVEAT. UCNI matter may be marked with the caveat "DISSEMINATION CONTROLLED" when programmatic requirements place special dissemination or reproduction limitations on information controlled as UCNI. This marking indicates that reproduction, extraction of information, or redistribution of such matter requires the permission of the cognizant DOE program office. If this caveat is applied, the originator must ensure that the following marking is placed immediately above the matter's front marking:

## DISSEMINATION CONTROLLED

Distribution authorized to DOE and DOE contractors only. Other requests shall be approved by the cognizant DOE program office, which is \_\_\_\_\_, before release.

5. **SPECIAL FORMAT MATTER.** Special formats of unclassified matter (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audio or videotapes, slides) must be marked to the extent practical as described in paragraphs 2 and 3, above. Regardless of the precise markings used in such cases, any special-format, unclassified matter that contains UCNI must be marked so that both a person in physical possession of the matter (e.g., markings on a viewgraph frame, a film reel and its container) and a person with access to the information in or on the matter (e.g., markings on the projected image of a slide, a warning on a film leader) are made aware that it contains UCNI. When space is limited, as on a 35-mm slide, the "UCNI" marking will suffice.
6. **TRANSMITTAL DOCUMENTS.** A document that (a) transmits matter marked as containing UCNI and (b) does not itself contain classified information or UCNI must be marked on its front as follows:

Matter transmitted contains Unclassified Controlled Nuclear Information. When separated from enclosures, this transmittal document does not contain UCNI.

7. **UNCLASSIFIED MATTER THAT NO LONGER CONTAINS UCNI.** A Reviewing Official or a Denying Official may determine that unclassified matter marked as containing UCNI no longer contains UCNI. In such a case, the official must ensure that all UCNI markings are removed or crossed out and that the front of the matter is marked as follows:

DOES NOT CONTAIN  
UNCLASSIFIED CONTROLLED  
NUCLEAR INFORMATION

Reviewing  
Official: \_\_\_\_\_  
(Name/Organization)  
Date: \_\_\_\_\_

8. **UNCLASSIFIED MATTER THAT DOES NOT CONTAIN UCNI.** A Reviewing Official may determine that unclassified, unmarked matter does not contain UCNI. No markings are required in such a case; however, for documentation purposes, the Reviewing Official may mark or may authorize the front of the matter to be marked with the same marking used in paragraph 7 above.

9. **UPGRADING.** A Reviewing or Denying Official may determine that existing, unmarked matter contains UCNI. The Reviewing or Denying Official making the determination must notify the originator or document custodian, providing sufficient information for the originator or document custodian to identify the specific matter being upgraded. This notification must itself be marked UCNI. To the extent practical, the originator or document custodian should notify all holders of the matter of the determination.

## CHAPTER II

### PROTECTION OF UCNI

1. ACCESS TO UCNI. Access to UCNI must be provided only to those authorized for routine or special access.
  - a. Routine Access. Routine access refers to the normal exchange of UCNI during the conduct of official business and allows for further dissemination of UCNI if the requirements in paragraph (2) below are met.
    - (1) Authorized Individual. An Authorized Individual, who may be the originator or possessor of UCNI, may grant routine access to UCNI to another person eligible for routine access to UCNI (see paragraph 1a(2) below) simply by giving that person UCNI. No explicit designation or security clearance is required. The recipient of the UCNI becomes an Authorized Individual for that specific UCNI. A Reviewing Official is an Authorized Individual for matter that the Reviewing Official determines to contain UCNI.
    - (2) Eligibility for Routine Access. To be granted routine access to UCNI, a person must need to know the specific UCNI in the performance of official duties or DOE-authorized activities. In addition to the need-to-know requirement, the person must meet at least one of the following requirements:
      - (a) U.S. Citizen. The person is a U.S. citizen who is one of the following:
        - 1 A Federal employee or member of the U.S. Armed Forces.
        - 2 An employee of a Federal contractor or subcontractor or an employee of a prospective Federal contractor or subcontractor who will use the UCNI for the purpose of bidding on a Federal contract or subcontract.
        - 3 A Federal consultant or DOE advisory committee member.
        - 4 A Member of Congress.
        - 5 A staff member of a congressional committee or of an individual Member of Congress.

- 6 The Governor of a state, his/her designated representative, or a State government official.
  - 7 A local government official or an Indian tribal government official.
  - 8 A member of a State, local, or Indian tribal law enforcement or emergency response organization.
- (b) Other Than a U.S. Citizen. The person is other than a U.S. citizen and is one of the following:
- 1 A Federal employee or a member of the U.S. Armed Forces.
  - 2 An employee of a Federal contractor or subcontractor.
  - 3 A Federal consultant or DOE advisory committee member.
- (c) Other Than a U.S. Citizen and Otherwise Not Eligible for Routine Access. The person may be other than a U.S. citizen who is not otherwise eligible for routine access to UCNI under the above paragraph, but who requires routine access to specific UCNI in conjunction with one of the following:
- 1 An international nuclear cooperative activity approved by the U.S. Government.
  - 2 U.S. diplomatic dealings with foreign government officials.
  - 3 An agreement for cooperation under section 123 of the Atomic Energy Act.
  - 4 Provisions of treaties, mutual defense acts, or Federal contracts or subcontracts.

The Authorized Individual who desires to release UCNI to a person for the reasons listed in this paragraph must coordinate such release with the DOE Secretarial Officer or NNSA Deputy Administrator or Chief with cognizance over the information. (For example, release of security-related UCNI at any site requires the approval of the Director of Safeguards and Security, not the program office that manages the site.)

- (3) Dissemination Limitations. An Authorized Individual may disseminate UCNI only to a person who is eligible for routine access to UCNI (see paragraph 1a(2) above) or to a person granted special access to UCNI (see paragraph 1b below).
  - (4) Access to UCNI Matter by Prospective Contractors in Bid Rooms. To have access to matter that contains UCNI in bid rooms, a prospective contractor desiring access must execute a self-certification that he/she is a U.S. citizen and will use the UCNI only in a manner consistent with the requirements in 10 CFR Part 1017. This self-certification must be sent to the local contracting office.
  - (5) Deviation from Requirements. The Office of Safeguards and Security may approve a waiver or recommend approval of an exception to any requirement for routine access to specific UCNI. However, the Office of Safeguards and Security must obtain the concurrence of the DOE Secretarial Officer or NNSA Deputy Administrator of Chief having cognizance over the UCNI prior to granting such a waiver for routine access to specific UCNI.
- b. Special Access. Special access may be granted to individuals not authorized for routine access to UCNI. For example, special access might be granted to an attorney representing an employee in litigation with DOE.
- (1) Submission of a Request. A person not authorized for routine access to UCNI may submit a request for special access to UCNI through the cognizant DOE or NNSA security office to the cognizant DOE Secretarial Officer or NNSA Deputy Administrator or Chief. Such a request must include the following:
    - (a) requester's name, current residence or business address, birthplace, birth date, and country of citizenship;
    - (b) a description of the UCNI requested;
    - (c) a description of the purpose for which the UCNI is needed; and
    - (d) certification by the requester of his/her understanding of, and willingness to abide by, the requirements in 10 CFR Part 1017.
  - (2) Granting a Request. The DOE Secretarial Officer or NNSA Deputy Administrator or Chief must base his/her decision to grant special access to UCNI on an evaluation of the following criteria:

- (a) the sensitivity of the UCNI for which special access is being requested (i.e., the worst-case, adverse effect on the health and safety of the public or the common defense and security that would result from unauthorized use of the UCNI);
  - (b) the purpose for which the UCNI is needed (e.g., will the UCNI be used for commercial or other private purposes or for public benefit to fulfill statutory or regulatory responsibilities);
  - (c) the likelihood of unauthorized dissemination by the requester; and
  - (d) the likelihood of the requester using the UCNI for illegal purposes.
- (3) Notification to the Office of Safeguards and Security. When special access is approved by the DOE Secretarial Officer or the NNSA Deputy Administrator or Chief, he/she must provide the Office of Safeguards and Security with the following information:
  - (a) name of individual granted special access,
  - (b) description of the UCNI,
  - (c) date of approval, and
  - (d) justification for granting the request.
- (4) Notification of Requester. Within 30 days of receipt of the request, the DOE Secretarial Officer or the NNSA Deputy Administrator or Chief must notify the requester of the determination or, if a determination cannot be made within 30 days, of the date when the determination will be made.
- (5) Special Access Limitations. A person granted special access to specific UCNI is not an Authorized Individual and must not further disseminate the UCNI.
- (6) Categorical Special Access Approval. A related group of individuals may be eligible for approval of special access to UCNI. In such a case, the relationship of the individuals must be described, but the individuals themselves need not be identified. (Example: All attorneys and paralegals of a law firm who are representing a client in a lawsuit against a DOE site.) Requests for such categorical special access approval are submitted to the Director of Safeguards and Security.
- (7) Notification of Responsibilities by Use of Cover Sheet. Each person granted special access to UCNI must be notified of applicable regulations concerning

UCNI prior to dissemination of the UCNI. Attaching DOE F 5639.1, "Unclassified Controlled Nuclear Information (UCNI) (Controlled)," to the front of the matter containing UCNI prior to its transmittal to the person constitutes notification.

2. **PHYSICAL PROTECTION REQUIREMENTS.** The following physical protection requirements apply to matter containing UCNI.
  - a. **Protection in Use.** An Authorized Individual must maintain physical control over any matter marked as containing UCNI to prevent unauthorized access to the information.
  - b. **Protection in Storage.** UCNI matter must be stored to preclude unauthorized disclosure. Storage of such matter with other unclassified matter in unlocked receptacles, such as file cabinets, desks, or bookcases, is adequate when Government or Government-contractor internal building security is provided during non-duty hours. When such internal building security is not provided, locked rooms or buildings provide adequate after-hours protection. If rooms or buildings are not locked or otherwise controlled, UCNI matter must be stored in locked receptacles, such as file cabinets, desks, or bookcases.
  - c. **Reproduction.** Matter marked as containing UCNI may be reproduced without permission of the originator to the minimum extent necessary consistent with the need to carry out official duties. The reproduced matter must be marked and protected in the same manner as the original matter. Copy machine malfunctions must be cleared and all paper paths checked for UCNI material. Excess paper containing UCNI must be destroyed as described below.
  - d. **Destruction.**
    - (1) At a minimum, UCNI matter must be destroyed by using strip cut shredders that result in particles of no more than ¼-inch wide strips. Other methods that provide sufficient destruction (e.g., an intact document buried in an onsite, controlled-access landfill) may be approved by the cognizant DOE security office.
    - (2) The decision to dispose of any DOE matter, whether or not it contains UCNI, must be consistent with the authorities for Federal records disposition which emanate solely from Departmental records disposition schedules (Standard Form 115) approved by the National Archives and Records Administration (NARA) or from the General Records Schedules published by NARA and applicable throughout the Government. The unauthorized destruction of Federal records is punishable under laws of the United States.

e. Transmission. Transmission must be by means that preclude unauthorized disclosure or dissemination.

(1) Outside a Facility.

- (a) Matter marked as containing UCNI must be packaged in a single, opaque envelope or wrapping.
- (b) Any of the following U.S. mail methods may be used: U.S. First Class, Express, Certified, or Registered Mail may be used.
- (c) Any commercial carrier may be used.
- (d) An Authorized Individual or a person granted special access may handcarry the matter as long as he/she can control access to the matter being transmitted.

(2) Within a Facility.

- (a) A standard distribution envelope, such as the U.S. Government Messenger Envelope (Optional Form No. 65-B) or equivalent, may be used.
- (b) An Authorized Individual or a person granted special access may handcarry the matter as long as he/she can control access to the matter being transmitted.

(3) Over Telecommunications Circuits. UCNI must be protected by encryption when transmitted by telecommunications services, including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities and radio communications. If UCNI is transmitted over public-switched broadcast communications paths (e.g., Internet) then the information must always be protected by encryption. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management").

Vertical line denotes change

Mission accomplishment may require the transmission of UCNI without encryption in emergency situations or when the sender or receiver requires the information for public safety or security purposes but does not have encryption capability. In such cases, approval to waive the encryption requirements must be obtained from (1) for Headquarters, the Director, Office of Headquarters Security Operations, Office of Security, or (2) for the field, the Operations Office Manager or Safeguards and Security Director. Such waivers are to be used only in situations where urgency precludes other more secure means of transmission. Absence of encryption capability does not justify routine unencrypted transmission of UCNI.

- f. Automated Information Systems (AIS). The AIS or AIS network must ensure that only personnel authorized for access to UCNI can access that information. For example, networks interconnected with a public-switched broadcast network (e.g., Internet) must provide methods (e.g., authentication, file access controls, etc.) to ensure that UCNI is protected against unauthorized access. UCNI being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide encryption in accordance with paragraph 2e(3) above to ensure that the information is not improperly accessed.

## CHAPTER III

### VIOLATIONS AND INFRACTIONS

1. **VIOLATIONS.** Violation means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of UCNI or any knowing willful, or negligent action to control information as UCNI for prohibited reasons (see 10 CFR 1017.5). Violations are reported under DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM. Heads of program and support offices within DOE and NNSA may recommend to the Office of Safeguards and Security the imposition of a civil or criminal penalty for a violation, as appropriate. The Director of Safeguards and Security must advise the Director of Security Affairs of each alleged violation. The Director of Security Affairs may recommend the Secretary impose a civil penalty or seek imposition of the criminal penalty by referring the matter to the Attorney General for investigation and prosecution.
2. **INFRACTIONS.** Infraction means any knowing, willful, or negligent action contrary to the requirements of this Manual that does not comprise a violation. A DOE employee who commits an infraction is subject to an administrative penalty, as outlined in DOE O 3750.1, WORK FORCE DISCIPLINE; a DOE contractor employee who commits such an infraction is subject to such penalty as the contractor may impose.

U.S. Department of Energy  
Washington, D.C.

PAGE CHANGE

DOE M 471.1-1 Chg 1

Approved: 06-30-00  
Chg 1: 10-23-01

SUBJECT: IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED  
NUCLEAR INFORMATION MANUAL

---

1. PURPOSE. To transmit revised pages to DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 06-30-00.
2. EXPLANATION OF CHANGES. To clarify when and how encryption requirements for Unclassified Controlled Nuclear Information may be waived.
3. FILING INSTRUCTIONS.

<u>Remove</u>	<u>Dated</u>	<u>Insert</u>	<u>Dated</u>
Page 6	06-30-00	Page 6	10-23-01
Page 7	06-30-00	Page 7	10-23-01

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:



FRANCIS S. BLAKE  
Deputy Secretary

---

DISTRIBUTION:  
All Departmental Elements

INITIATED BY:  
Office of Security and Emergency  
Operations

**U.S. Department of Energy**  
Washington, D.C.

**ORDER**

**DOE O 471.2A**

Approved: 03-27-97  
Sunset Review: 09-26-97  
Expires: 09-26-99

**SUBJECT: INFORMATION SECURITY PROGRAM**

**1. OBJECTIVES.**

- a. To establish an Information Security Program for the protection and control of classified and sensitive information. The Information Security Program includes the following programs.
  - (1) Operations Security (OPSEC).
  - (2) Classified Matter Protection and Control (CMPC).
  - (3) Classified Information Systems Security (ISS).
  - (4) Technical Surveillance Countermeasures (TSCM).
  - (5) Security of Foreign Intelligence Information (FII) and Sensitive Compartmented Information (SCI).
  - (6) Security of Special Access Programs (SAP).
  - (7) Protection of Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), and Naval Nuclear Propulsion Information.
- b. To ensure that individuals protect classified information and sensitive unclassified information to which they have access or custody.
- c. To ensure that classified information is not released to the public until it has been formally and officially declassified by an appropriate declassification authority and its release is otherwise permitted by applicable law or regulation. Likewise, no sensitive unclassified information shall be released without review for applicable release restrictions.
- d. To establish protection systems that require higher degrees of protection for each higher classification level (Confidential, Secret, Top Secret).

Vertical Line Denotes Change.

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Office of Safeguards and Security

2. **CANCELLATIONS.** The Orders listed below are canceled. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with such an Order. Canceled Orders which are incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Orders.
- a. DOE 5630.8A, SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION, of 7-31-90.
  - b. DOE 5639.1, INFORMATION SECURITY PROGRAM, of 10-19-92.
  - c. DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92.
  - d. DOE 5639.6A, CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM, of 7-15-94.
  - e. DOE 5639.7, OPERATIONS SECURITY PROGRAM, of 4-30-92.
  - f. DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94, Chapter III, paragraphs 1, 2, and 4 through 9.
3. **APPLICABILITY.**
- a. **General.** This Order applies to Departmental Elements responsible for protection and control of classified information and sensitive unclassified information.
  - b. **Application to Contracts.** Except as excluded in paragraph 3c below, this Order applies to covered contractors (a DOE contractor or subcontractor subject to DOE Acquisition Regulation, Part 952.204-2, or other clause requiring protection of classified information, nuclear material, or other sensitive information or activities). Contractor requirements are listed in the Contractor Requirements Document, Attachment 1. The Contractor Requirements Document is issued to aid procurement request initiators in identifying requirements that are to be incorporated into contracts by contracting officers.
  - c. **Exclusion.** Requirements of this Order that overlap or duplicate requirements of the Nuclear Regulatory Commission related to radiological emergency planning do not apply to the design, construction, operation, and decommissioning of Office of Civilian Radioactive Waste Management facilities.

Vertical Line Denotes Change.

4. REQUIREMENTS.

a. Access to Classified and Sensitive Unclassified Information.

- (1) Access to classified information shall be granted only to persons who possess the appropriate access authorization and need-to-know according to DOE O 472.1, PERSONNEL SECURITY PROGRAM. Supervisors or other responsible officials who are knowledgeable about the classified information and the responsibilities of the individual may determine need-to-know. The individual disseminating classified information is responsible for ensuring that the recipient of the information has the appropriate access authorization and need-to-know.
- (2) Before a facility is eligible for access to classified information, a DOE facility clearance must be granted according to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.
- (3) Access to sensitive unclassified information shall be granted only to persons who possess the appropriate need-to-know. The individual disseminating sensitive unclassified information is responsible for determining the recipient's need-to-know. Access to Naval Nuclear Propulsion Information shall only be granted to U.S. citizens who have a need-to-know.
- (4) Owners of data are responsible for determining the sensitivity of information before it is used, processed, or stored on information systems and for ensuring the system is accredited for the information to be used in it.
- (5) Classified and unclassified Naval Nuclear Propulsion Information shall be protected in accordance with Naval Sea Systems Command Instruction C5511.32B, dated 12-22-93. Naval Nuclear Propulsion Information shall be protected pursuant to export control requirements and statute. Questions regarding Naval Nuclear Propulsion Information shall be directed to the Deputy Assistant Secretary for Naval Reactors.

b. Classified Information Systems. Security requirements for classified information systems contained in this Order and DOE M 5639.6A-1 are to be implemented as follows.

- (1) Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this Order and DOE M 5639.6A-1. These systems must meet the requirements of this Order and DOE M 5639.6A-1 no later than July 15, 1997.
- (2) Classified information systems in the process of accreditation on July 15, 1994, may be accredited under DOE 5639.6A; however, the requirements of this Order and DOE M 5639.6A-1 must be met by these systems no later than January 15, 1996.

Vertical Line Denotes Change.

(3) New classified information systems that are under development and that have not begun certification and security performance testing shall meet the requirements of this Order and DOE M 5639.6A-1.

- c. Implementation Plans. Implementation plans are necessary only for requirements that cannot be implemented with existing resources or within 6 months of the effective date of this Order. These plans shall be developed within 90 days of the effective date of this Order and submitted to the Office of Safeguards and Security. Implementation plans shall ensure that full implementation of this Order is accomplished within 1 year of the effective date of the Order.
- d. Deviations. Unless otherwise stated in this Order, deviations from the requirements in this Order shall be processed according to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.
- e. Supplementary Directives. The following Manuals supplement this Order and contain non-discretionary, mandatory Information Security Program requirements, standards, and procedures.
- (1) DOE M 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL.
  - (2) DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM.
  - (3) DOE "Technical Surveillance Countermeasures Procedural Manual," (classified).
- f. Guides. The following Guides shall be maintained by the Office of Safeguards and Security to provide discretionary, non-mandatory assistance in implementing the requirements of the above Manuals and this Order:
- (1) DOE G 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL, and
  - (2) "DOE OPSEC Procedural Guide."
- g. Definitions. Terms commonly used in the program are defined in the "Safeguards and Security Definitions Guide," which is maintained and distributed by the Office of Safeguards and Security.

## 5. RESPONSIBILITIES AND AUTHORITIES.

### a. Heads of Departmental Elements.

- (1) Designate an individual(s) to be responsible for bringing to the attention of the contracting officer the applicable requirements in the Contractor Requirements Document, including supporting details, for each procurement. Unless another

individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization").

- (2) Develop and submit implementing plans as required.
- (3) In coordination with the Director of Security Affairs, approve the release of SECRET and CONFIDENTIAL information within their programmatic areas of responsibility, originated by DOE or contractors, to other Government agencies and their contractors, to foreign governments, and to international organizations, as deemed appropriate.
- (4) Approve the distribution of classified scientific and technical reports within their programmatic areas of responsibility.
- (5) Ensure the protection of other Federal agencies' classified matter with at least those precautions prescribed for DOE information of the same classification.
- (6) Send classified information containing Restricted Data and/or Formerly Restricted Data that is to be provided to foreign entities to the Deputy Assistant Secretary for Facility Transition and Technical Support, who will channel the information to the Joint Atomic Information Exchange Group (JAIEG) for review prior to release.
- (7) Ensure that upon completion of work under contract, subcontract, or other agreement, a review of classified matter associated with that effort is accomplished to reduce the volume of classified matter insofar as practical and that proper authorizations, if applicable, are obtained for the elimination or retention of such matter.

b. Managers of Operations Offices and Field Offices, and Director, Headquarters Operations Division, Office of Safeguards and Security.

- (1) Ensure the designation and appointment of TOP SECRET control officers and alternates as custodians and notify Headquarters, Office of Safeguards and Security, of the selection and position titles of the designees.
- (2) Request the approval of the Headquarters Office of Safeguards and Security for DOE and contractor employees on official Departmental business to hand-carry classified matter to and from foreign countries.
- (3) Serve as the Designated Accrediting Authority (DAA) in coordination with the Classified Computer Security Program Manager, for classified information systems under their cognizance to be operated at a Protection Index of five, as defined in DOE M 5639.6A-1. This authority may not be redelegated.
- (4) Appoint, in coordination with the Computer Security Program Manager, a senior-level DOE employee as the DAA, for classified information systems under their cognizance to be operated at a Protection Index of three.

- (5) Appoint a Computer Security Operations Manager who will also serve as the DAA for classified computer systems under their cognizance to be operated at a Protection Index of zero, one, or two and to oversee classified information systems security programs at DOE and DOE-contractor facilities under their cognizance.
- (6) Ensure the Headquarters Operations Division and each DOE Field Element, contractor, or subcontractor under their cognizance appoints a Classified Information Systems Security Site Manager, responsible to their management and to the CSOM for the implementation of Classified Information Systems Security within their organizations.
- (7) Through each manager or supervisor responsible for a classified information system, ensure the following:
  - (a) Appointment of a Classified Computer Systems Security Officer (CSSO), either a DOE or covered contractor employee, for each classified information system at a facility and identification of that individual in the Classified Information Systems Security Plan. An individual may serve as the Classified System Security Officer for one or more classified information systems.
  - (b) Computer System Security Officer for each classified Information System is aware of and fulfills his/her duties as described in this Order and DOE M 5639.6A-1.
- (8) Designate an OPSEC Manager, a CMPC Operations Manager, a TSCM Operations Manager, and a Special Access Program (SAP) Security Coordinator. These managers, for their assigned area(s) of responsibility, shall accomplish the following:
  - (a) Ensure the implementation of DOE policy and procedures.
  - (b) Develop and implement local policy and procedures.
  - (c) Conduct appropriate surveys and self-assessments to ensure effective implementation.
  - (d) Review the results of surveys and self-assessments for lessons learned and trends analysis.
- (9) Ensure facilities included in the Operations Security program develop and maintain Operations Security plans, procedures, and program files to assist in implementing an active program, and approve these plans and procedures, as appropriate.
- (10) Ensure issuance of infractions, when required, to DOE and DOE-contractor personnel.

Vertical Line Denotes Change.

c. Director of Nonproliferation and National Security.

- (1) Determines (in coordination with the Director of Central Intelligence for intelligence information) whether sharing classified information with foreign governments will result in a net advantage to the national security of the United States.
- (2) Establishes agreements, in coordination with other appropriate agencies, for sharing classified information with foreign governments.
- (3) Obtains security assurances for the proposed exchange of classified information with foreign governments.
- (4) Implements Chapter V of this Order for establishing nuclear, intelligence, acquisition, operations and support, law enforcement, and emergency operations-related SAPs.
- (5) Authorizes specific DOE organizations and covered contractors to create and retain information designated as Protect as Restricted Data (PARD).

d. Director of Energy Intelligence.

- (1) Exercises authorities vested in the Secretary by the Director of Central Intelligence in furtherance of the provisions of Executive Order 12958, sections 3.5© and 3.6(e).
- (2) Accredits DOE and DOE-contractor Sensitive Compartmented Information Facilities.
- (3) Approves access to FII and SCI for DOE and DOE contractor personnel.
- (4) Controls use and dissemination of FII and SCI by DOE and DOE contractor personnel.
- (5) Functions as the Department's point-of-contact involving activities related to intelligence and counterintelligence, to include oversight of program access to intelligence information provided to, or originated within, DOE. Coordinates with the Office of Security Affairs concerning security issues, to include espionage and the possible or potential compromise of intelligence-related information.
- (6) Serves as the DAA for classified information systems that process intelligence information and are located in Sensitive Compartmented Information Facilities.
- (7) Establishes, as necessary, policy and procedures, beyond those described in this Order and DOE M 5639.6A-1, for processing classified intelligence information in Sensitive Compartmented Information Facilities, in coordination with the Classified Information System Security Program Manager.
- (8) Processes National Security Council matter containing SCI received and dispatched from DOE.

e. Director of Security Affairs.

- (1) Acts as the Senior Agency Official responsible for the direction and administration of the Information Security Program.
- (2) Exercises authorities vested in the Secretary under Executive Order 12958 and implementing directives, except the following.
  - (a) The authority in the Executive Order, section 4.4, pertaining to the creation of SAPs.
  - (b) Authority delegated to the Secretary by the Director of Central Intelligence in the Executive Order, sections 3.5.(c) and 3.6(e).
- (3) Advises and assists DOE and DOE contractors in implementing information security programs.
- (4) Ensures other Government agencies and foreign governments are informed of any potential compromise of their information.
- (5) Through the Director of Safeguards and Security.
  - (a) Administers and oversees implementation of the Atomic Energy Act of 1954, as amended, for the protection of Restricted Data and Formerly Restricted Data.
  - (b) Administers and oversees implementation of Executive Order 12958, "Classified National Security Information," pertaining to SAPs, personnel, and physical security requirements for the control and protection of National Security Information.
  - (c) Designates DOE Information Security Program Managers. These managers shall be DOE employees who are highly knowledgeable in their specialty. They are appointed to manage elements of the Information Security Program and shall be designated as the OPSEC Program Manager, Classified Information Systems Security Program Manager, Classified Matter Protection and Control Program Manager, Technical Surveillance Countermeasures Program Manager, and Special Access Program Security Program Manager (excluding intelligence SAP program security managers). These managers, for their assigned areas of responsibility, shall accomplish the following:
    - (1) Represents the DOE on national-level committees.

Vertical Line Denotes Change.

- (2) Develops policies, standards, and procedures.
- (3) Directs safeguards and security technology development efforts as required.
- (4) Provides advice and guidance to Information Security Operations Managers at Field Elements in implementing the program.
- (5) Oversees the development of information security training courses.
- (6) Periodically assesses the effectiveness of the program.
- (7) Ensures compliance with security-related reporting requirements of Federal or legislative directives and provides details of unauthorized disclosures to the Information Security Oversight Office.

(d) Ensures the establishment of an Independent Validation and Verification capability to be made available to DOE site and facility managers.

(e) Ensures the development and implementation of an Information Security training program meeting the requirements of DOE O 470.1.

(f) Establishes accreditation criteria for classified AIS systems.

f. Assistant Secretary for Human Resources and Administration.

- (1) Develops policy and provides oversight for the implementation of the TEMPEST, Protected Distribution System (PDS), Communications Security (COMSEC), and Unclassified Computer Security Programs for the Department.
- (2) Assists the Director of Security Affairs, as needed, during the Internal Review Budget process by ensuring that integrated security systems are planned, designed, and constructed.
- (3) Assists the Director of Security Affairs during the conduct of certifications, reviews, surveys, and program reviews of Information Security Programs.
- (4) Represents the Department as a member of the National Security Telecommunications Information Systems Security Committee.
- (5) Provides advice and assistance in determining solutions to correct any telecommunications vulnerabilities detected by safeguards and security activities.

Vertical Line Denotes Change.

- (6) Designates the Headquarters Classified Information System Security Site Manager for classified information systems in Headquarters Elements in the Washington metropolitan area.
  - (7) Processes all National Security Council matter received and dispatched by DOE, with the exception of matter that contains SCI, or matter submitted by the National Security Council or other Federal agencies to the Office of Declassification for classification review.
  - (8) Processes all classified matter for the Secretary, Deputy Secretary, and Under Secretary.
  - (9) Establishes the DAA structure for the Department.
- g. Assistant Secretary for Defense Programs.
- (1) Implements Chapter V of this Order for establishing defense-related SAPs.
  - (2) Through the Deputy Assistant Secretary for Facility Transition and Technical Support.
    - (a) Develops policy and requirements and executes approvals and delegations of authority for controlling access to weapon data according to DOE 5610.2, CONTROL OF WEAPON DATA, of 8-1-80.
    - (b) For unaccounted-for classified matter or compromised classified information, coordinates the required reporting to the Joint Atomic Information Exchange Group.
    - (c) Channels all matters containing Restricted Data or Formerly Restricted Data being sent to foreign entities to the Joint Atomic Information Exchange Group (JAIEG) for review prior to release.
- h. Director for Nuclear Energy shall implement Chapter V of this Order for establishing nuclear energy-related SAPs.
- I. Director Naval Nuclear Propulsion Program shall implement and oversee all policy and practices pertaining to Information Security for activities under the Director's cognizance.
- j. Procurement Request Originators (the individuals responsible for initiating a requirement on DOE F 4200.33 or other individual(s) designated by the cognizant Head of Departmental Element) shall bring to the attention of the cognizant contracting officer:

Vertical Line Denotes Change.

- (1) each procurement to which elements of the Contractor Requirements Document apply, and
  - (2) elements of the Contractor Requirement Document that apply to any subcontract or subaward.
- k. Contracting Officers shall, based on advice received from the procurement request originator or other designated individuals, apply pertinent requirements in the Contractor Requirements Document to awards falling within its scope. For awards other than management and operating contracts, this shall be by incorporation or reference using explicit language in a contractual action.
6. CONTACT. Questions concerning this Order should be directed to Technical and Operations Security of the Policy, Standards, and Analysis Division, Office of Safeguards and Security, at 301-903-2528.

BY ORDER OF THE SECRETARY OF ENERGY:



ARCHER L. DURHAM  
Assistant Secretary for Human  
Resources and Administration

TABLE OF CONTENTS

	<u>Page</u>
<u>CHAPTER I - PROGRAM MANAGEMENT</u> .....	I-1
1. Security Organization .....	I-1
2. Security Infractions .....	I-1
3. Unaccounted For Matter and Compromise of Classified Information .....	I-2
<u>CHAPTER II - OPERATIONS SECURITY PROGRAM</u> .....	II-1
1. Objectives .....	II-1
2. Applicability .....	II-1
3. Requirements .....	II-1
<u>CHAPTER III - CLASSIFIED INFORMATION SYSTEMS SECURITY</u> .....	III-1
1. Objective .....	III-1
2. Applicability .....	III-1
3. Requirements .....	III-1
<u>CHAPTER IV - PROTECTION AND CONTROL OF CLASSIFIED MATTER</u> .....	IV-1
1. Objectives .....	IV-1
2. Applicability .....	IV-1
3. Requirements .....	IV-1
<u>CHAPTER V - SPECIAL ACCESS PROGRAMS</u> .....	V-1
1. Objectives .....	V-1
2. Applicability .....	V-1
3. Requirements .....	V-1
Attachment 1 - Contractor Requirements Document	

## CHAPTER I

### PROGRAM MANAGEMENT

1. **SECURITY ORGANIZATION.** To ensure an effective information security program, the following requirements shall be implemented.
  - a. A clear chain of responsibility for information security shall exist within each organization.
  - b. Qualified personnel and other resources shall be available to implement and maintain the information security program.
  - c. Individuals responsible for managing or implementing information security programs shall be provided adequate time and resources to satisfactorily accomplish assigned functions in accordance with applicable directives.
  - d. Information security training shall be developed and implemented, as necessary.
  - e. Heads of Departmental Elements responsible for programs requiring protection and control of classified and/or sensitive unclassified information shall ensure that plans are established and approved by the cognizant security office prior to initiation of such programs.
  - f. Management shall be involved in and supportive of all aspects of information security. This involvement and support shall be demonstrated by regular visits to and inspections of information security operations to ensure that operations meet existing standards and policies.
  - g. Management shall ensure that information security is included and documented in protection program planning documents. Site-specific characteristics shall be considered and documented to ensure that information is properly controlled.
  
2. **SECURITY INFRACTIONS.** An infraction is any knowing, willful, or negligent action contrary to the requirements of this Order that does not constitute a violation of law or result in the actual compromise or the unauthorized disclosure of classified information. Requirements for handling violations are contained in DOE O 470.1.
  - a. **Report of Security Infraction.** DOE F 5639.3, "Report of Security Incident/Infraction," or a similar form shall be used to document infractions and a copy of the report kept in

Vertical Line Denotes Change.

the employee's official DOE personnel security file. With each occurrence, security practices or procedures shall be reviewed and revised, if necessary, to preclude recurrence.

- b. Records of Security Infractions. The safeguards and security organization or officer reporting the security infraction and the cognizant Departmental Element shall maintain records of each infraction.
- c. Disciplinary or Corrective Actions.
  - (1) For DOE employees, disciplinary or corrective action shall be determined by the Heads of Departmental Elements in coordination with the Office of Personnel. Any disciplinary or adverse action involving a DOE employee shall be according to DOE 3750.1, WORK FORCE DISCIPLINE, of 3-23-83.
  - (2) For contractor employees, disciplinary or corrective action shall be determined by appropriate management officials according to the contractor's personnel policies and procedures.
  - (3) For military personnel and employees of other Government agencies assigned to DOE or DOE contractors, DOE or its contractors shall take corrective action and submit a report of infraction to the military organization or Government agency to which the employee is permanently assigned for whatever disciplinary action that the cognizant agency or organization deems necessary.

3. UNACCOUNTED FOR MATTER AND COMPROMISE OF CLASSIFIED INFORMATION. Loss, compromise, or unauthorized disclosure of information and unaccounted-for matter shall be handled according to DOE O 470.1 and DOE M 471.2-1. In addition, the following requirements apply.

- a. Discovery. Any person who determines that classified matter has been or may have been lost or compromised or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and immediately report this information to the facility security officer.
- b. Inspection. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection of the area where the matter was stored, handled, or processed shall be conducted. Custodians providing support to the holder must be queried. When applicable, the accountability records shall be audited for evidence of destruction, transmission, or other disposition. The inspection and query process shall be completed within 48 hours.
- c. Inquiry. When inspection efforts fail to reconcile unaccounted for matter, and for all potential compromises, the appointed Inquiry Official shall initiate an inquiry. The DOE safeguards and security organization shall advise the Office of Safeguards and Security of the initiation of an inquiry.

- d. Damage Assessments.
- (1) Purpose. Damage assessments to assess potential damage to national security are required by 32 CFR, Chapter XX, Part 2000, "National Security Information," Section 2001.47 "Loss or Possible Compromise." Damage assessments are used by responsible managers to determine future courses of action within the program and by security personnel to evaluate possible countermeasures and cover actions to limit potential damage.
  - (2) When Required. When the inquiries disclose evidence that information may have been compromised and the compromise can reasonably be expected to cause damage to the national security, a damage assessment shall be conducted. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, loss of classified information, unaccounted for classified matter, or through various other circumstances. Both circumstances of the loss and sensitivity of the information must be considered in determining when a damage assessment is required.
- e. Notification to Information Security Oversight Office. On receiving written confirmation from a Departmental Element of an unauthorized disclosure of, or access to, National Security Information by a DOE employee, DOE contractor, or consultant, the Office of Safeguards and Security shall notify the Information Security Oversight Office of the details. Such notification shall be given immediately when the disclosure results from systematic problems. Otherwise, semiannual reports of unauthorized disclosures shall be made.
- f. Records Retention. Records of all actions pertaining to unaccounted for/compromised matter or compromises of classified information must be maintained by the facility security officer and the cognizant Departmental Element safeguards and security organization. Records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.

## CHAPTER II

### OPERATIONS SECURITY PROGRAM

1. **OBJECTIVES.** The objective of the OPSEC Program is to help ensure that sensitive information is protected from compromise and secured against unauthorized disclosure. The program is structured to provide management with the necessary information required for sound risk management decisions concerning the protection of sensitive information. OPSEC techniques and measures shall be utilized throughout the Department to achieve this objective. The counterimagery program shall be an integral part of the OPSEC Program pertaining to imagery-susceptible, sensitive activities.
2. **APPLICABILITY.** This section applies only to facilities possessing sensitive information, whether classified or unclassified, for which adequate OPSEC is required to detect and deter efforts to illegally gain access to that information. As determined by the cognizant Department authority, the amount and sensitivity of information, balanced against its vulnerability and attractiveness, will be considered when calculating the level of OPSEC activities required.
3. **REQUIREMENTS.** To meet the objectives of the OPSEC Program, the organization shall accomplish the following.
  - a. Develop and maintain OPSEC plans, procedures, and program files. OPSEC plans will include, at a minimum, goals, milestones, and, where applicable, an annex describing actions to identify and counter imagery collection from air- and space-borne platforms, OPSEC plans shall be reviewed and updated as required on an annual basis; a memorandum reflecting completion of this action will be placed in the OPSEC files.
  - b. Establish a sufficient number of OPSEC working groups to perform the necessary management and support functions required for an effective OPSEC program, to include OPSEC education and awareness. Working groups shall develop and set priorities for their OPSEC program objectives consistent with approved plans and policies, meet on a regular basis, and maintain meeting records, a copy of which shall be held by the responsible OPSEC Manager.
  - c. Prepare a threat statement that describes the local OPSEC threat and develop a Critical Sensitive Information List (CSIL) and supporting Essential Elements of Friendly Information (EEFI), which will be appropriately classified, set according to priorities, and disseminated to cognizant managers for review, comment, and action based on the adequacy of countermeasures in place at each site. The threat statement and CSIL/EEFI will be reviewed by the cognizant OPSEC Working Group and senior Headquarters' program management and updated at least annually. The results of such reviews will be recorded in OPSEC managers' files.
  - d. Conduct OPSEC assessments of all facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program and falling within their

purview. OPSEC assessments will be conducted at other facilities involved in the creating, handling, storing, processing, or transmission of sensitive information, whether classified or unclassified, as deemed necessary by the cognizant Department authority. A copy of these assessments, to include observations, recommendations, and actions taken, will be provided to the Office of Safeguards and Security for historical purposes.

- (1) Either the programmatic or facility approach may be used to conduct the OPSEC assessment. If the facility approach is used, all activities at the facility will be included in the assessment. If the programmatic approach is used, all activities within the individual program will be included in the assessment. Priority of effort for the assessment should be based on the Critical and Sensitive Information List, threat assessment, risk management concepts, and direction from management.
  - (2) Effective immediately, facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program will conduct an OPSEC assessment at least every 3 years, or sooner if the facility environment changes significantly. If the programmatic approach is used and more than one major program is located at the facility, a schedule will be developed and implemented that provides for the conduct of a minimum of one programmatic assessment annually. Major programs will be identified by the local Working Group.
- e. Conduct an OPSEC review of all sensitive activities and facilities whenever:
- (1) new construction is planned for a facility that will process or store classified or sensitive information or matter;
  - (2) new sensitive activities are initiated or significant changes occur to existing programs; or
  - (3) a sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding 2 years.
- f. Conduct OPSEC liaison with other Field Elements and local agencies. Advise the Office of Safeguards and Security of broadly based OPSEC initiatives involving these organizations.
- g. Analyze the results of OPSEC assessments and, in consonance with risk management, develop and implement countermeasures, as appropriate.
- h. Conduct an initial review of all ongoing sensitive activities to identify those susceptible to imaging exploitation.
- i. Report annually, on November 1st, to the Office of Safeguards and Security and applicable program officials on the status of the OPSEC Program for the preceding fiscal year.

- j. Ensure that OPSEC responsibilities for Work For Others programs to the extent specified in the basic contract or Memorandum of Understanding are fulfilled. Primary responsibility for OPSEC activity within any Work for Others program rests with the Work for Others Program Manager. Any OPSEC interaction between the Work for Others program and the local OPSEC program will be as mutually agreed between the Work for Others Program Manager and the cognizant OPSEC Manager.

## CHAPTER III

### CLASSIFIED INFORMATION SYSTEMS SECURITY

1. **OBJECTIVE.** To ensure classified information and unclassified information processed on classified information systems are protected against unauthorized disclosure or compromise.
2. **APPLICABILITY.** Systems requiring this protection include but are not limited to the following.
  - a. Mainframe classified information systems, word processors, microprocessors, personal computers, programmable controllers, automated office support systems, memory typewriters, and other stand-alone or special systems that process, store, transfer, or provide access to classified information, including those classified information systems that also process, store, transfer, or provide concurrent access to both classified and unclassified information.
  - b. Special purpose computers that perform classified functions and/or contain classified data, such as numerically controlled machines, smart switches, single-task preprogrammed controllers, programmable facsimile devices, automated testers, and digital-to-analog and analog-to-digital converters.
  - c. Networks wherein classified information is processed, stored, transferred, or accessed in one or more components of the network.
3. **REQUIREMENTS.** *This Order and DOE M 5639.6A-1 shall be used with other DOE directives to provide a comprehensive protection program for classified Information Systems. These directives establish minimum requirements for the design, procurement, and implementation of information systems that process, store, transfer, or provide access to classified information. Unclassified information processed on classified information systems is subject to the requirements of this Order and DOE M 5639.6A-1, unless processed under period processing procedures. If processing of only unclassified information takes place during period processing, the information processed is subject to DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 1-7-93.*
  - a. **Protection of Classified Information and Resources.** The Classified Information Systems Security Program shall be implemented to ensure the following.
    - (1) The integrity of the information on the classified information system is preserved.
    - (2) Information processed on the classified information system is protected from unauthorized access, alteration, modification, disclosure, transmission, or destruction.

- (3) The classified information system's resources provide an appropriate level of protection against denial of service, subversion of security measures, or improper use.
  - (4) The classified information system's resources are protected from damage, destruction, and unauthorized modification.
- b. Protection Measures. All reasonable measures shall be used to protect information systems that process, store, transfer, or provide access to classified information. These measures include but are not limited to the following.
- (1) Measures related to personnel security, physical security, telecommunications security, administrative security, technical security, and hardware and software security shall be used to protect information on the classified information system to result in an acceptable level of risk against loss, improper use, compromise, or unauthorized alteration or modification of classified information.
  - (2) Acquisitions or other procurement actions to obtain information system equipment or related contractual services (as defined in DOE 1360.1B) that will be used to process, store, transfer, or provide access to classified information shall be:
    - (a) evaluated by the Classified Information System Security Site Manager to ensure that appropriate security technology is being specified and
    - (b) integrated into the Information Resources Management Long Range Plan according to DOE 1360.1B.
  - (3) Information Systems used to process, store, transfer, or provide access to classified information shall meet the following requirements.
    - (a) Accredited by a DAA to be operated:
      - (1) in a particular mode of operation as defined in DOE M 5639.6A-1;
      - (2) with a prescribed set of personnel, administrative, operational, physical, telecommunications, hardware, software, and technical requirements;
      - (3) under a stated operational concept; and
      - (4) with identified interconnections to other information systems.
    - (b) Reaccredited by a DAA at least once every 3 years except classified information systems processing SCI.
    - (c) Covered by a continuity of operations decision or a plan (see DOE M 5639.6A-1, Chapter I, paragraph 9).

- (d) Operated under the oversight of a designated Departmental or covered contractor manager or supervisor.
- (e) Accessed only by personnel who have:
  - (1) received training in their security responsibilities;
  - (2) a proper level of access authorization and need-to-know; and
  - (3) acknowledged in writing their responsibilities to protect information on classified information systems.
- c. Information Systems Containing Intelligence Information. The requirements of this Order and DOE M 5639.6A-1 apply to classified information systems that process classified intelligence information within a Sensitive Compartmented Information Facility. However, these requirements may not fully represent the protection requirements for processing intelligence information; further requirements may be established by directives of the intelligence community.
- d. Baseline for Protection. This Order and DOE M 5639.6A-1 provide a uniform baseline for the protection of classified information systems. Each DAA, as described in this Order and DOE M 5639.6A-1, is responsible for ensuring that the security requirements of this Order and DOE M 5639.6A-1 are met for each classified information system that he/she accredits.

## CHAPTER IV

### PROTECTION AND CONTROL OF CLASSIFIED MATTER

1. **OBJECTIVES.** To establish a system of procedures, facilities, and equipment to protect and control classified matter that is being generated, received, transmitted, used, stored, reproduced, or destroyed.
  - a. To establish a system of procedures to provide an adequate audit trail for all accountable classified matter.
  - b. To establish a control system geared to providing controls based on classification category (Restricted Data, Formerly Restricted Data, or National Security Information) or special handling instructions or caveats.
2. **APPLICABILITY.** This section applies only to facilities that have classified matter.
3. **REQUIREMENTS.**
  - a. Classification level and category shall be used in determining the degree of protection and control required to prevent unauthorized access to classified matter.
  - b. Controls shall be established to detect and deter unauthorized access to classified matter.
  - c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.
  - d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent unauthorized visual and/or aural access.
  - e. Classified information and sensitive unclassified information shall be disclosed to contractors pursuant to an authorized and legitimate U.S. government requirement only.
  - f. Detailed requirements for marking, accountability and control systems, reproduction, receipt, transmission, and destruction are contained in DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
  - g. **Emergency Procedures.** Procedures shall be developed for safeguarding classified matter in emergency situations.

Vertical Line Denotes Change.

## CHAPTER V

### SPECIAL ACCESS PROGRAMS

1. **OBJECTIVES.** To establish requirements for and limit the types of SAPs authorized for use within the Department. Authorized SAPs are categorized as acquisition, operations and support, and intelligence SAPs. Terms and activities such as Limited Access Program, Controlled Access Program, and Limited Distribution Programs are not authorized.
2. **APPLICABILITY.** This section applies only to facilities that provide oversight for, operate, or host special access programs.
3. **REQUIREMENTS.** All DOE-originated SAPs must be approved by the Secretary, with the recommendation of the Deputy Secretary, who serves as the Chairperson of the Special Access Programs Oversight Committee, which oversees the development of policy and procedures for SAPs.
  - a. Security policy and procedures for DOE SAPs are developed by the Office of Safeguards and Security, in coordination with the appropriate Program Office.
  - b. DOE and Non-DOE (Work-For-Others) SAPs, with the exception of intelligence SAPs, are registered through the established Facility Data and Approval Record process (see DOE O 470.1). The Facility Data and Approval Record will be classified in accordance with "Classification Guide for Safeguards and Security Information" (CG-SS-3), Chapter II. DOE SAPs are registered with the SAP Security Program Manager. Intelligence SAPs are registered with the Office of Energy Intelligence.
  - c. SAP facilities and activities will be surveyed according to DOE O 470.1 by the cognizant Operations Office and/or Office of Safeguards and Security, in coordination with the appropriate Program Office and/or sponsor. Intelligence SAPs are inspected by the Office of Energy Intelligence.
  - d. Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies.
  - e. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be immediately reported to the appropriate Program Office and the Director of Safeguards and Security, according to established Departmental policies.

**CONTRACTOR REQUIREMENTS DOCUMENT**  
**INFORMATION SECURITY PROGRAM**

1. This contractor requirement document is issued to aid procurement request initiators to identify requirements that are to be incorporated into contracts by contracting officers. The following requirements are based on statutes, Executive Orders, and national directives that are designed to deter unauthorized access to classified information and sensitive unclassified information.  
  
The contractor is responsible for protecting classified and sensitive unclassified information and shall ensure the following:
  - a. That individuals protect classified information and sensitive unclassified information to which they have access or custody.
  - b. That classified information is not released to the public until it has been formally and officially declassified by an appropriate declassification authority and its release is otherwise permitted by applicable law or regulation. Likewise, no sensitive unclassified information shall be released without review for applicable release restrictions.
  - c. That protection systems that require higher degrees of protection be established for each higher classification level (Confidential, Secret, Top Secret).
  - d. That provisions of this CRD flow down to all subcontractors with responsibilities for protecting classified and sensitive unclassified information.
  
2. General Requirements. Access to classified information shall be granted only to persons who possess the appropriate need-to-know and access authorization in accordance with applicable DOE directives and the Manual for Personnel Security Activities when issued. Supervisors or other responsible officials who are knowledgeable of the classified information and the responsibilities of the individual may determine need-to-know. The individual disseminating classified information is responsible for ensuring that the recipient of the information has the appropriate access authorization and need-to-know. Additionally, the contractor shall accomplish the following:
  - a. Obtain a DOE facility clearance before a facility is eligible for access to classified information.
  - b. Ensure access to sensitive unclassified information is granted only to persons who possess the appropriate need-to-know. The individual disseminating sensitive unclassified information is responsible for determining the recipient's need-to-know. Access to Naval

Vertical Line Denotes Change.

Nuclear Propulsion Information shall only be granted to U.S. citizens who have a need-to-know.

- c. Ensure that owners of data are responsible for determining the sensitivity of information before it is used, processed, or stored on information systems and for ensuring the system is accredited for the information to be used in it.
  - d. Ensure classified and unclassified Naval Nuclear Propulsion Information is protected in accordance with Naval Sea Systems Command Instruction C5511.32B, dated 12-22-93. Naval Nuclear Propulsion Information shall be protected pursuant to export control requirements and statute. Questions regarding Naval Nuclear Propulsion Information shall be directed to the Deputy Assistant Secretary for Naval Reactors.
3. Classified Information Systems (ISS) Security requirements for classified information systems contained in this CRD and DOE M 5639.6A-1 shall be implemented as follows.
- a. Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this CRD and DOE M 5639.6A-1. These systems must meet the requirements of this CRD and DOE M 5639.6A-1 no later than July 15, 1997.
  - b. Classified information systems in the process of accreditation on July 15, 1995 may be accredited; however, the requirements of this CRD and DOE M 5639.6A-1 must be met by these systems no later than January 15, 1996.
  - c. New classified information systems that are under development, and that have not begun certification and security performance testing, shall meet the requirements of this CRD and DOE M 5639.6A-1.
4. Supplementary Directives. The following Manuals supplement this CRD and contain non-discretionary, mandatory Information Security Program requirements, standards, and procedures.
- a. DOE M 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL.
  - b. DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM.
  - c. DOE "Technical Surveillance Countermeasures Procedural Manual" (classified).
5. Program Management. To ensure an effective information security program, the contractor shall accomplish the following:
- a. Maintain a clear chain of responsibility for information security within each organization.

- b. Ensure that qualified personnel and other resources are available to implement and maintain the information security program.
- c. Provide adequate time and resources to individuals responsible for managing or implementing information security programs to satisfactorily accomplish assigned functions.
- d. Ensure information security training is developed and implemented, as necessary.
- e. Ensure programs requiring protection and control of classified and/or sensitive unclassified information have plans established and approved by the cognizant security office prior to initiation of such programs.
- f. Have programs that are unclassified, but potentially sensitive, receive a timely review by the appropriate OPSEC Working Group. Once a determination has been made that sensitive information is involved, the identity of the information shall be forwarded to the cognizant security office.
- g. Ensure management is involved in and supports of all aspects of information security. This involvement and support shall be demonstrated by regular visits to and inspections of information security operations to ensure that operations meet existing standards and policies.
- h. Ensure that information security is included and documented in protection program planning documents. Site-specific characteristics shall be considered and documented to ensure that information is properly controlled.

6. Security Infractions.

- a. Use DOE F 5639.3, "Report of Security Incident/Infraction," or a similar form to document infractions and forward a copy of the report to DOE. With each occurrence, security practices or procedures shall be reviewed and revised, if necessary, to preclude recurrence.
- b. Ensure the safeguards and security organization or officer reporting the security infraction maintains records of each infraction.
- c. Administer disciplinary or corrective actions as follows.
  - (1) For contractor employees, disciplinary or corrective action shall be determined by appropriate management officials according to the contractor's personnel policies and procedures.

Vertical Line Denotes Change.

- (2) For military personnel and employees of other Government agencies assigned to DOE contractors, DOE or its contractors shall take corrective action and submit a report of infraction to the military organization or Government agency to which the employee is permanently assigned for whatever disciplinary action that the cognizant agency or organization deems necessary.
7. Unaccounted For Matter and Compromise of Classified Information. Loss, compromise, or unauthorized disclosure of information and unaccounted-for matter shall be handled according to DOE O 470.1 and DOE M 471.2-1. In addition, the following requirements shall apply.
  - a. Any person who determines that classified matter has been or may have been lost or compromised or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and immediately report this information to the facility security officer.
  - b. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection shall be completed within 48 hours.
  - c. When inspection efforts fail to reconcile unaccounted for matter, and for all potential compromises, the appointed Inquiry Official shall initiate an inquiry and ensure notification to DOE.
  - d. Records Retention. Records of all actions pertaining to unaccounted for/compromised matter or compromises of classified information must be maintained by the facility security officer. Records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.
8. Operations Security. To meet the objectives of the Operations Security Program, the organization shall accomplish the following.
  - a. Develop and maintain Operations Security plans, procedures, and program files. Operations Security plans will include, at a minimum, goals, milestones, and, where applicable, an annex describing actions to identify and counter imagery collection from air- and space-borne platforms. Operations Security plans shall be reviewed and updated as required on an annual basis; a memorandum reflecting completion of this action will be placed in the Operations Security files.
  - b. Establish a sufficient number of Operations Security working groups to perform the necessary management and support functions required for an effective Operations Security program, to include Operations Security education and awareness. Working groups shall develop and set priorities for their Operations Security program objectives consistent with approved plans and policies, meet on a regular basis, and maintain meeting records, a copy of which shall be held by the responsible Operations Security Manager.

- c. Prepare a threat statement that describes the local Operations Security threat and develop a Critical Sensitive Information List (CSIL) and supporting Essential Elements of Friendly Information (EEFI), which will be appropriately classified, set according to priorities, and disseminated to cognizant managers for review, comment, and action based on the adequacy of countermeasures in place at each site. The threat statement and CSIL/EEFI will be reviewed by the cognizant Operations Security Working Group and senior Headquarters' program management and updated at least annually. The results of such reviews will be recorded in Operations Security managers' files.
- d. Conduct Operations Security assessments of all facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program falling within their purview. OPSEC assessments will be conducted at other facilities involved in creating, handling, storing, processing, or transmitting sensitive information, whether classified or unclassified, as deemed necessary by the cognizant Department authority. A copy of these assessments, to include observations, recommendations, and actions taken, will be provided to the Office of Safeguards and Security for historical purposes.
  - (1) Either the programmatic or facility approach may be used to conduct the OPSEC assessment. If the facility approach is used, all activities at the facility will be included in the assessment. If the programmatic approach is used, all activities within the individual program will be included in the assessment. Priority of effort for the assessment should be based on the Critical and Sensitive Information List, threat assessment, risk management concepts, and direction from management.
  - (2) Effective immediately, facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program will conduct an OPSEC assessment at least every 3 years, or sooner if the facility environment changes significantly. If the programmatic approach is used and there is more than one major program located at the facility, a schedule will be developed and implemented that provides for the conduct of a minimum of one programmatic assessment annually. Major programs will be identified by the local Working Group.
- e. Conduct an OPSEC review of all sensitive activities and facilities whenever:
  - (1) new construction is planned for a facility that will process or store classified or sensitive information or matter;
  - (2) new sensitive activities are initiated or significant changes occur to existing programs; or
  - (3) a sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the proceeding 2 years.

- f. Conduct Operations Security liaison with local agencies. Advise the Office of Safeguards and Security of broadly based Operations Security initiatives involving these organizations.
  - g. Analyze the results of Operations Security assessments and, in consonance with risk management, develop and implement countermeasures, as appropriate.
  - h. Conduct an initial review of all ongoing sensitive activities to identify those susceptible to imaging exploitation.
  - i. Report annually, on October 1st, to the cognizant DOE field office Safeguards and Security Director on the status of Operations Security Program for the preceding fiscal year.
  - j. Ensure that Operations Security responsibilities for Work For Others programs are fulfilled to the extent specified in the basic contract or Memorandum of Understanding.
9. Classified Information Systems Security. The Classified Information Systems Security Program shall be implemented to ensure the following.
- a. The integrity of the information on the classified information system is preserved.
  - b. Information processed on the classified information system is protected from unauthorized access, alteration, modification, disclosure, transmission, or destruction.
  - c. The classified information system's resources provide an appropriate level of protection against denial of service, subversion of security measures, or improper use.
  - d. The classified information system's resources are protected from damage, destruction, and unauthorized modification.
  - e. All reasonable measures shall be used to protect information systems that process, store, transfer, or provide access to classified information. These measures include but are not limited to the following.
    - (1) Measures related to personnel security, physical security, telecommunications security, administrative security, technical security, and hardware and software security shall be used to protect information on the classified information system to result in an acceptable level of risk against loss, improper use, compromise, or unauthorized alteration or modification of classified information.
    - (2) Acquisitions or other procurement actions to obtain information system equipment or related contractual services that will be used to process, store, transfer, or provide access to classified information shall be:

- (a) evaluated by the Classified Information System Security Site Manager to ensure that appropriate security technology is being specified and
  - (b) integrated into the Information Resources Management Long Range Plan.
- (3) Information Systems used to process, store, transfer, or provide access to classified information shall meet the following requirements.
- (a) Accredited by a DAA to be operated:
    - 1 in a particular mode of operation as defined in DOE M 5639.6A-1;
    - 2 with a prescribed set of personnel, administrative, operational, physical, telecommunications, hardware, software, and technical requirements;
    - 3 under a stated operational concept; and
    - 4 with identified interconnections to other information systems.
  - (b) Reaccredited by a DAA at least once every 3 years except classified information systems processing SCI.
  - (c) Covered by a continuity of operations decision or a plan (see Chapter I, paragraph 9, DOE M 5639.6A-1).
  - (d) Operated under the oversight of a designated Departmental or covered contractor manager or supervisor.
  - (e) Accessed only by personnel who have:
    - 1 received training in their security responsibilities;
    - 2 a proper level of access authorization and need-to-know; and
    - 3 acknowledged in writing their responsibilities to protect information on classified information systems.

f. Information Systems Containing Intelligence Information. The requirements of this CRD and DOE M 5639.6A-1 apply to classified information systems that process classified intelligence information within a SCIF. However, these requirements may not fully represent the protection requirements for processing intelligence information; further requirements may be established by directives of the intelligence community.

- g. Baseline for Protection. This CRD and DOE M 5639.6A-1 provide a uniform baseline for the protection of classified information systems. Each Designated Accrediting Authority, as described in this CRD and DOE M 5639.6A-1, is responsible for ensuring that the security requirements are met for each classified information system accredited.
10. Protection and Control of Classified Matter. The contractor will establish a system of procedures, facilities, and equipment to protect and control classified matter that is being generated, received, transmitted, used, stored, reproduced, or destroyed. Note: This section only applies only to facilities with have classified matter. The following provisions shall apply.
- a. Classification level and category shall be used in determining the degree of protection and control required to prevent unauthorized access to classified matter.
  - b. Controls shall be established to detect and deter unauthorized access to classified matter.
  - c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.
  - d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent unauthorized visual and/or aural access.
  - e. Classified information and sensitive unclassified information shall be disclosed to contractors pursuant to an authorized and legitimate U.S. government requirement only.
  - f. Detailed requirements for Classified Matter Protection and Control will be implemented as mandated in DOE M 471.2-1.
  - g. Emergency Procedures. Procedures shall be developed for safeguarding classified matter in emergency situations.
11. Special Access Programs. Contractors will notify the local DOE SAP Security Coordinator prior to acceptance of all non-DOE SAPs.
- a. Contractors shall ensure that protection program planning documents, including security plans and standard operating procedures, comply with established SAP policies.
  - b. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be immediately reported to the appropriate Program Office and the Director of Safeguards and Security, according to established Departmental policies.

Vertical Line Denotes Change.

U.S. Department of Energy  
Washington, D.C.

ORDER

DOE O 471.3

Approved: 4-9-03  
Sunset Review: 4-9-05  
Expires: 4-9-07

SUBJECT: IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

1. OBJECTIVE. To establish a program within the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), to identify certain unclassified controlled information as Official Use Only (OUO) and to identify, mark, and protect documents containing such information. This information may be exempt from public release under the Freedom of Information Act (FOIA) and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities.
2. CANCELLATION. None.
3. APPLICABILITY.
  - a. DOE Elements. Except as noted in paragraph 3c, this Order applies to all DOE elements, including NNSA, listed on Attachment 1 that (1) identify information under their cognizance as OUO and mark documents they generate accordingly or (2) possess documents that are marked as containing OUO information or with equivalent markings from other agencies (see definitions for examples of such markings).
  - b. Contractors.
    - (1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that apply to contractors responsible for the management and operation of the Department-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.
    - (2) This CRD must be included in site/facility management contracts that involve activities where OUO information and documents will be handled, used, or generated.
    - (3) The officials identified in paragraph 5, Responsibilities, are responsible for notifying the contracting officers which site/facility management contracts are affected. Once notified, the contracting officer is responsible for incorporating the CRD into each affected site/facility management contract via the Laws, Regulations, and Departmental Directives clause of the contract.

DISTRIBUTION:  
All Departmental Elements

INITIATED BY:  
Security Policy Staff Office of Security

(4) As the Laws, Regulations, and Departmental Directives clause of a site/facility management contract states, regardless of the performer of the work, the site/facility management contractor with the CRD incorporated into its contract is responsible for compliance with the requirements of the CRD. An affected site/facility management contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

- c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, the Director of the Naval Nuclear Propulsion Program will determine the applicability of this Order for activities and facilities under his control.

#### 4. REQUIREMENTS.

- a. To be identified as OUO, information must be unclassified; have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities; and fall under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive order). (See DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03, for additional details.)
- b. An unclassified document originated within a program element must be evaluated to determine whether it contains OUO information. An unclassified document that is produced by or for DOE/NNSA or is under the control of DOE/NNSA may be evaluated to determine whether it contains OUO information. (NOTE: Documents maintained in restricted access files do not need to be reviewed while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. See DOE M 471.3-1, Chapter 1, for additional details.)
- c. A document determined to contain OUO information must be marked as described in DOE M 471.3-1. (NOTE: Documents maintained in restricted access files do not need to be marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. See DOE M 471.3-1, Chapter I, paragraph 4e.)
- d. A document determined to no longer warrant protection as OUO must have its markings removed as described in DOE M 471.3-1.

- e. Access to (1) documents marked as containing OOU information or (2) OOU information from such documents must only be provided to those persons who need to know the information to perform their jobs or other DOE-authorized activities.
- f. Documents marked as containing OOU information and other-Agency documents with equivalent markings must be protected as described in DOE M 471.3-1.
- g. An administrative penalty as prescribed in DOE 3750.1, *Work Force Discipline*, dated 3-23-83, is imposed if an employee (1) intentionally releases OOU information from a document marked as containing OOU information to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (2) intentionally or negligently releases a document marked as containing OOU information to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (3) intentionally does not mark a document that is known to contain OOU information, or (4) intentionally marks a document that is known not to contain OOU information.
- h. If a document marked as containing OOU information is requested under FOIA, the document is not automatically exempt from public release, but must be reviewed and processed under 10 CFR Part 1004.
- i. Except for Unclassified Controlled Nuclear Information, which is identified, marked, and protected under DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 6-30-00, and Naval Nuclear Propulsion Information, which is controlled under 32 CFR Part 250, OOU markings are the only markings to be used within DOE to designate documents containing unclassified controlled information. Additional markings that are based on law, regulation, or other DOE directives that convey additional advice on handling or access restrictions (e.g., "Source Selection Information—See FAR 2-101 and 3.104"; "Protected CRADA Information"; "Export Controlled Information") are allowed.

5. RESPONSIBILITIES.

- a. Secretarial Officers.
  - (1) Review procurement requests for new site/facility management contracts and, if appropriate, ensure that the requirements of the CRD of this directive are included in the contracts.
  - (2) Ensure that requirements contained in paragraph 4 of this Order are implemented by employees within their respective organizations.

- (3) May develop and approve guidance to be used by all employees to identify documents containing OUO information under their cognizance and forward such guidance to the Director, Office of Security, for issuance.
      - (4) May develop, approve, and issue guidance to be used only by employees within their respective organizations to identify documents containing OUO information. Such guidance must be consistent with guidance issued under paragraphs 5a(3) and 5b(2).
    - b. Director, Office of Security.
      - (1) Develops and issues policies and procedures to identify OUO information and to identify and mark documents containing such information.
      - (2) Develops and issues guidance, with the concurrence of the program office with cognizance over the information, to assist individuals in determining whether a document contains OUO information. Issues guidance for use by all DOE employees that was developed and approved by Secretarial officers under paragraph 5a(3).
      - (3) Develops and issues protection requirements for OUO information.
      - (4) Develops and disseminates training material and conducts training sessions to assist individuals in identifying documents containing OUO information and marking such documents.
    - c. Freedom of Information Officers. Coordinate requests for documents under FOIA.
    - d. Contracting Officers.
      - (1) After notification by the appropriate program official, incorporate the CRD into the affected site/facility management contract in accordance with the Laws, Regulations, and DOE Directives clause of the contracts.
      - (2) Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Order in new non site/facility management contracts, as appropriate.
  6. DEVIATIONS FROM REQUIREMENTS. A Secretarial Officer may propose a variance (i.e., an alternate or equivalent means of meeting a requirement) or request a waiver from a specific requirement in this Order or in DOE M 471.3-1. This proposal must (a) identify the Order or Manual requirement for which a variance or waiver is being requested; (b) explain why a variance or waiver is needed; and (c) if requesting a variance, describe the alternate or equivalent means for meeting the requirement. The

proposal must be submitted to the Director, Office of Security, for approval. The Director's decision must be made within 30 days. The Office of Security will review each approved variance or waiver periodically to ensure it is still needed.

7. REFERENCES.

- a. 10 CFR Part 1004, Freedom of Information.
- b. DOE O 241.1A, *Scientific and Technical Information Management*, dated 4-9-01.
- c. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.
- d. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.
- e. DOE 3750.1, *Work Force Discipline*, dated 3-23-83.

8. DEFINITIONS.

- a. Document. Recorded information regardless of its medium or characteristics.
- b. Equivalent markings. Other-Agency information control markings that are equivalent to DOE Official Use Only (OUO) include but are not limited to the following: "For Official Use Only" (FOUO) from the Department of Defense and many other agencies, "Sensitive But Unclassified" (SBU) from the Department of State, and "Limited Official Use" (LOU) from the Department of Justice.
- c. Information. Facts, data, or knowledge itself regardless of the medium of its conveyance. (Documents are deemed to convey or contain information and are not considered to be information per se.)
- d. Official Use Only (OUO) information. Certain unclassified information that may be exempt from public release under the Freedom of Information Act and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities.

9. CONTACT. Questions concerning this Order should be addressed to Information Classification and Control Policy at 301-903-5454.

BY ORDER OF THE SECRETARY OF ENERGY:



KYLE E. McSLARROW  
Deputy Secretary

**DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE O 471.3,  
*Identifying and Protecting Official Use Only Information, IS APPLICABLE***

Office of the Secretary  
Office of the Chief Information Officer  
Office of Civilian Radioactive Waste Management  
Office of Congressional and Intergovernmental Affairs  
Office of Counterintelligence  
Departmental Representative to the Defense Nuclear Facilities Safety Board  
Office of Economic Impact and Diversity  
Office of Energy Efficiency and Renewable Energy  
Energy Information Administration  
Office of Environment, Safety and Health  
Office of Environmental Management  
Office of Fossil Energy  
Office of General Counsel  
Office of Hearings and Appeals  
Office of Independent Oversight and Performance Assurance  
Office of the Inspector General  
Office of Intelligence  
Office of Management, Budget and Evaluation and Chief Financial Officer  
National Nuclear Security Administration  
Office of Nuclear Energy, Science and Technology  
Office of Policy and International Affairs  
Office of Public Affairs  
Office of Science  
Secretary of Energy Advisory Board  
Office of Security  
Office of Worker and Community Transition  
Office of Energy Assurance  
Bonneville Power Administration  
Southeastern Power Administration  
Southwestern Power Administration  
Western Area Power Administration

**CONTRACTOR REQUIREMENTS DOCUMENT**  
**DOE O 471.3, *Identifying Official Use Only Information***

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. The contractor shall:

1. Determine whether unclassified documents created and/or handled in the performance of this contract contain Official Use Only (OUO) information. (See Chapter I, paragraphs 2a and 2b, of the CRD for DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.)
2. Ensure that documents determined to contain OUO information are marked appropriately. (See Chapter I, paragraph 4, of the CRD for DOE M 471.3-1.) Except for Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI), OUO markings are the only markings to be used to designate documents containing unclassified controlled information. Additional markings that are based on law, regulation, or other DOE CRD that convey additional advice on handling or access restrictions (e.g., "Protected CRADA Information," "Export Controlled Information") are allowed.
3. Ensure that documents determined to no longer warrant protection as OUO have their markings removed. [See Chapter I, paragraphs 4g(1) and 4g(2) of the CRD for DOE M 471.3-1.]
4. Ensure that access to (a) documents marked as containing OUO information or (b) OUO information from such documents is only provided to those persons who need to know the information to perform their jobs or other DOE-authorized activities.
5. Ensure that documents marked as containing OUO information and other-Agency documents with equivalent markings [e.g., "For Official Use Only" (FOUO) from the Department of Defense; "Sensitive But Unclassified" (SBU) from the Department of State; "Limited Official Use" (LOU) from the Department of Justice] are protected. (See Chapter II, paragraph 2, of the CRD for DOE M 471.3-1.)
6. Ensure that a request for a variance (i.e., an alternate or equivalent means of meeting a requirement) or waiver from any requirements in the CRD for DOE O 471.3 or DOE M 471.3-1 are provided to the appropriate Secretarial Officer. Such request must (a) identify the requirement for which a variance or waiver is being requested; (b) explain why the variance or waiver is needed; and (c) if requesting a variance, describe the alternate or equivalent means for meeting the requirement.

7. Impose an administrative penalty, as appropriate, if (a) OOU information from a document marked as containing OOU information is intentionally released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (b) a document marked as containing OOU information is intentionally or negligently released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities, (c) a document that is known to contain OOU information is intentionally not marked, or (d) a document that is known to not contain OOU information is intentionally marked as containing such information.

DOE M 471.3-1

Approved: 4-9-03  
Sunset Review: 4-9-05  
Expires: 4-9-07

# MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

---



**U.S. DEPARTMENT OF ENERGY**  
Office of Security

---

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Security Policy Staff

## MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

---

1. PURPOSE. This Department of Energy (DOE) Manual provides detailed requirements to supplement DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.
2. SUMMARY. This Manual comprises two chapters that provide direction for identifying, marking, and protecting Official Use Only (OUO) information. These chapters address mandatory procedures and management processes. Chapter I describes the requirements for identifying and marking OUO information; Chapter II addresses protecting OUO information. The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that apply to site/facility management contractors.
3. REFERENCES.
  - a. 10 CFR Part 1004, Freedom of Information.
  - b. DOE O 241.1A, *Scientific and Technical Information*, dated 4-9-01.
  - c. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.
  - d. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.
  - e. DOE 3750.1, *Work Force Discipline*, dated 3-23-83.
4. CONTACT. Questions concerning this Manual should be addressed to Information Classification and Control Policy at 301-903-5454.

BY ORDER OF THE SECRETARY OF ENERGY:



KYLE E. McSLARROW  
Deputy Secretary

**CONTENTS**

**CHAPTER I. IDENTIFYING AND MARKING OFFICIAL USE ONLY INFORMATION I-1**

- 1. Identifying Information as Official Use Only ..... I-1
- 2. Determining Whether a Document Contains Official Use Only Information ..... I-1
- 3. Marking a Document that Contains Official Use Only Information ..... I-2

**CHAPTER II. PROTECTING OFFICIAL USE ONLY INFORMATION ..... II-1**

- 1. Access to Official Use Only Information ..... II-1
- 2. Physical Protection Requirements ..... II-1

## CHAPTER I

### IDENTIFYING AND MARKING OFFICIAL USE ONLY INFORMATION

1. IDENTIFYING INFORMATION AS OFFICIAL USE ONLY. To be identified as OOU, information must be unclassified and meet both of the following criteria:
  - a. Have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.
  - b. Fall under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OOU because it covers information classified by Executive order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests (see DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03, for a discussion of FOIA exemptions 2 through 9).
2. DETERMINING WHETHER A DOCUMENT CONTAINS OFFICIAL USE ONLY INFORMATION. An unclassified document that is originated within a DOE/NNSA office, produced by or for that office, or under the control of that office may contain OOU information. Any employee from an office with cognizance over such information may determine whether such a document contains OOU information. The process is as follows:
  - a. The employee first considers whether the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities.
  - b. If the information is considered to have the potential for such damage, then the employee consults guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3. If the specific information in question is identified as OOU information in such guidance, then the employee determines that the document contains OOU information.
  - c. If the information is considered to have the potential for such damage, but no guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3 covers the specific information in question, then the employee considers whether the information falls under at least one of FOIA exemptions 2 through 9 (consult the DOE G 471.3-1 for assistance in determining whether any of the exemptions apply). If the employee believes that the information falls under one of the FOIA

exemptions, then the employee may determine that the document contains OOU information.

- d. If the employee finds no basis for identifying the information as OOU in guidance issued under DOE O 471.3 and does not believe the information falls under one of the FOIA exemptions, then the employee must not mark the document as containing OOU information.

3. MARKING A DOCUMENT THAT CONTAINS OFFICIAL USE ONLY INFORMATION.

- a. Front Marking. The front marking includes the applicable FOIA exemption number and related category name (i.e., Exemption 2 - Circumvention of Statute; Exemption 3 - Statutory Exemption; Exemption 4 - Commercial/Proprietary; Exemption 5 - Privileged Information; Exemption 6 - Personal Privacy; Exemption 7 - Law Enforcement; Exemption 8 - Financial Institutions; Exemption 9 - Wells) and the name and organization of the employee making the determination and identifies the guidance used if the determination was based on guidance. (NOTE: The guidance referred to here is guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3, not the DOE directives guide (DOE G 471.3-1).) The employee making the determination ensures that the following marking is placed on the front of each document containing OOU information.

<b>OFFICIAL USE ONLY</b>	
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____	
Department of Energy review required before public release	
Name/Org: _____	Date: _____
Guidance (if applicable) _____	

- b. Page Marking. The employee making the determination must ensure that the words "Official Use Only" (or "OOU" if space is limited) are placed on the bottom of each page or, if more convenient, on just those pages containing the OOU information.
- c. Marking E-mail Messages. The first line of an e-mail message containing OOU information must contain the abbreviation "OOU" before the beginning of the text. If the message itself is not OOU but an attachment contains OOU information, the message must indicate that the attachment is OOU. The attachment must have all required OOU markings.
- d. Marking Special Format Documents. Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes,

videotapes, DVDs, or CD-ROMs) must be marked in a manner consistent with paragraphs 3a and 3b above so persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OOU information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.

- e. Marking Documents Maintained in Restricted Access Files. Documents that may contain OOU information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OOU information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OOU information and, if appropriate, marked. (NOTE: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.
- f. Transmittal Document. A document that (1) transmits an attachment or enclosure marked as containing OOU information and (2) does not itself contain classified or controlled information must be marked on its front as follows to call attention to the presence of OOU information in the attachments or enclosures.

Document transmitted contains OOU information
--

- g. Removal of Official Use Only Markings.
- (1) Markings Applied Based on Guidance. OOU markings applied based on guidance may be removed by any employee when the guidance used to make the determination states that the information is no longer OOU. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OOU. Once those deficiencies have been corrected, the OOU marking may be removed.)
- (2) Markings Applied Based on Employee's Evaluation. OOU markings applied based on an employee's evaluation may be removed by (1) the employee who initially applied the marking, (2) the supervisor of the employee who initially applied the marking, or (3) a FOIA authorizing official who approves the release of the document in response to a request made under FOIA.

Whoever makes the determination to remove the markings ensures that the markings are crossed out or otherwise obliterated and places the following marking on the bottom of the front of the document:

<p>DOES NOT CONTAIN OFFICIAL USE ONLY INFORMATION</p> <p>Name/Org.: _____ Date: _____</p>
---

- h. Relationship of Official Use Only Markings to Other Types of Control Markings.
- (1) Unclassified Documents. The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking [e.g., Unclassified Controlled Nuclear Information (UCNI)].
  - (2) Classified Documents. OUO front and page markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.
- i. Marking Documents Generated Before the Date of this Manual. Unclassified documents generated before the date of this Manual are not required to be reviewed to determine whether they contain OUO information unless they are to be publicly released. Any such previously generated document determined to contain OUO information after the date of this Manual must be marked as indicated in paragraph 3 above. Such determination may be made by anyone in the organization that currently has cognizance over the information in the document. In addition, for unclassified documents marked as containing OUO information before the date of this Manual, the markings are not required to be updated to conform with the marking requirements in this Manual.
- j. Obsolete Markings. From July 18, 1949, to October 22, 1951, the Atomic Energy Commission used the term "Official Use Only" as a designation for certain classified information. Documents from this time period with an OUO marking must be handled as Confidential National Security Information pending a determination of their proper classification. Refer to DOE M 475.1-1A, *Identifying Classified Information*, dated 5-8-98 [National Nuclear Security Administration (NNSA) certified 2-26-01], for specific procedures.

## CHAPTER II

### PROTECTING OFFICIAL USE ONLY INFORMATION

1. ACCESS TO OFFICIAL USE ONLY INFORMATION. Access to (a) documents marked as containing OOU information and (b) OOU information from such documents must only be provided to those persons who require the information to perform their jobs or other DOE-authorized activities. The responsibility for determining whether someone has a valid need for such access rests with the person who has authorized possession, knowledge, or control of the information or document and not on the prospective recipient.
2. PHYSICAL PROTECTION REQUIREMENTS.
  - a. Protection in Use. Reasonable precautions must be taken to prevent access to documents marked as containing OOU information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read an OOU document in a public place, such as a cafeteria, on public transportation).
  - b. Protection in Storage. Documents marked as containing OOU information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during non-duty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).
  - c. Reproduction. Documents marked as containing OOU information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OOU information. Excess paper containing OOU information must be destroyed as described below.
  - d. Destruction. A document marked as containing OOU information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office. The decision to dispose of any DOE or NNSA document, whether it contains OOU information or not, must be consistent with the policies and procedures for records disposition.

e. Transmission.

- (1) By Mail—Outside of a Facility.
  - (a) Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."
  - (b) Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.
  - (c) Any commercial carrier may be used.
- (2) By Mail—Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.
- (3) By Hand—Between Facilities or Within a Facility. A document marked as containing OOU information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.
- (4) Over Telecommunications Circuits. Documents marked as containing OOU should be protected by encryption when transmitted over telecommunications circuits whenever possible. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards (e.g., Entrust) that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.
  - (a) By Unencrypted Facsimile. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.
  - (b) By E-mail without Encryption. If encryption is not available and some form of protection is desired, the OOU information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.

- f. Transmission over Voice Circuits. OOU information transmitted over voice circuits should be protected by encryption (see DOE M 200.1-1, Chapter 9, for requirements) whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.
  
- g. Processing on Automated Information Systems. An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OOU information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

## CONTRACTOR REQUIREMENTS DOCUMENT

### DOE M 471.3-1, MANUAL FOR IDENTIFYING AND PROTECTING OFFICIAL USE ONLY INFORMATION

Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this Contractor Requirements Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. The contractor must:

1. Ensure that unclassified information meeting both of the following requirements is identified as OUO information.
  - a. The information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.
  - b. The information falls under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests (see Chapter II of the DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03, for a discussion of FOIA exemptions 2 through 9).
2. Ensure that unclassified documents originated by the contractor, produced by or for the contractor, or under the control of the contractor that have the potential to damage governmental, commercial, or private interests are identified as containing OUO information based on (a) guidance issued by the DOE, (b) guidance developed by the contractor that is consistent with guidance issued by the DOE, or (c) consideration that the information meets the criterion contained in paragraph 1b.
3. Ensure that a document containing OUO information is marked as follows:
  - a. Front Marking. The front marking includes the applicable FOIA exemption number and related category name (i.e., Exemption 2 - Circumvention of Statute; Exemption 3 - Statutory Exemption; Exemption 4 - Commercial/Proprietary; Exemption 5 - Privileged Information; Exemption 6 - Personal Privacy; Exemption 7 - Law Enforcement; Exemption 8 - Financial Institutions; Exemption 9 - Wells), the name and organization of the employee making the determination, and identifies the guidance used if the determination was based on guidance. [NOTE: The guidance referred to here is guidance issued by the DOE,

not the DOE directives guide (DOE G 471.3-1).] This marking is placed on the front of each document containing OUO information:

<b>OFFICIAL USE ONLY</b>	
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____	
Department of Energy review required before public release	
Name/Org: _____	Date: _____
Guidance (if applicable) _____	

- b. Page Marking. The words "Official Use Only" (or "OUO" if space is limited) are placed on the bottom of each page or, if more convenient, on just those pages containing the OUO information.
- c. Marking E-mail Messages. The first line of an e-mail message containing OUO information must contain the abbreviation "OUO" before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.
- d. Marking Special Format Documents. Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, DVDs, or CD-ROMs) must be marked in a manner consistent with paragraphs 3a and 3b above so persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OUO information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.
- e. Marking Documents Maintained in Restricted Access Files. Documents that may contain OUO information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked. (NOTE: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel controls to this order are in place.
- f. Transmittal Document. A document that (a) transmits an attachment or enclosure marked as containing OUO information and (b) does not itself contain classified

or controlled information must be marked on its front as follows to call attention to the presence of OUO information in the attachments or enclosures:

Document transmitted contains OUO information
--

4. Remove OUO markings from a document when it no longer warrants such protection. OUO markings applied based on guidance issued by DOE may be removed when the guidance used to make the determination states that the information is no longer OUO. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OUO. Once those deficiencies have been corrected, the OUO marking may be removed.)
5. Comply with the following marking requirements for documents containing OUO information and other types of classified or controlled information:
  - a. Unclassified Documents. The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking [e.g., Unclassified Controlled Nuclear Information (UCNI)].
  - b. Classified Documents. OUO markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.
6. Not require unclassified documents generated before the date of this CRD to be reviewed to determine whether they contain OUO information unless they are to be publicly released. Any such previously generated document determined to contain OUO information after the date of this CRD must be marked as indicated in paragraph 3 above. Such determination may be made by anyone with cognizance over the information in the document. In addition, for unclassified documents marked as containing OUO information before the date of this CRD, the markings are not required to be updated to conform with the marking requirements in this CRD.
7. Be cognizant of the fact that from July 18, 1949, to October 22, 1951, the Atomic Energy Commission used the term "Official Use Only" as a designation for certain classified information. Documents from this time period with an OUO marking must be handled as Confidential National Security Information pending a determination of their proper classification. (See Chapter V, Part B, paragraph 8d, of the CRD for DOE M 475.1-1A, *Identifying Classified Information*, dated 5-8-98 [National Nuclear Security Administration (NNSA) certified 2-26-01], for specific procedures.

8. Ensure that access to (a) documents marked as containing OUO information or (b) OUO information from such documents is provided only to those persons who need to know the information to perform their jobs or other DOE-authorized activities.
9. Ensure that the following protection requirements are followed:
  - a. Protection in Use. Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read an OUO document in a public place, such as a cafeteria, on public transportation, etc.).
  - b. Protection in Storage. Documents marked as containing OUO information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during nonduty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).
  - c. Reproduction. Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. Excess paper containing OUO information must be destroyed as described below.
  - d. Destruction. A document marked as containing OUO information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office. The decision to dispose of any DOE or NNSA document, whether it contains OUO information or not, must be consistent with the policies and procedures for records disposition.
  - e. Transmission.
    - (1) By Mail—Outside of a Facility.
      - (a) Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."
      - (b) Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.
      - (c) Any commercial carrier may be used.

- (2) By Mail—Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.
  - (3) By Hand—Between Facilities or Within a Facility. A document marked as containing OOU information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.
  - (4) Over Telecommunications Circuits. Documents marked as containing OOU should be protected by encryption when transmitted over telecommunications circuits whenever possible. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards (e.g., Entrust) that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.
    - (a) By Unencrypted Facsimile. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.
    - (b) By E-mail without Encryption. If encryption is not available and some form of protection is desired, the OOU information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.
- f. Transmission over Voice Circuits. OOU information transmitted over voice circuits should be protected by encryption (see DOE M 200.1-1, Chapter 9, for requirements) whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.
- g. Processing on Automated Information Systems. An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OOU information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

**DOE M 475.1-1A**

**2/26/01**

**THIS PAGE IS TO REMAIN WITH DOE M 475.1-1A**

**THE ONLY ADMINISTRATIVE CHANGES THAT OCCURRED IN  
THIS REVISION WERE-**

- 1. NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA),  
AND**
- 2. TO UPDATE ORGANIZATIONS TITLES.**

DOE M 475.1-1A

Approved: 5-8-98  
NNSA Certified: 2-26-01  
Sunset Review: 2-26-03  
Expires: 2-26-05

# IDENTIFYING CLASSIFIED INFORMATION

---



**U.S. DEPARTMENT OF ENERGY**  
**Office of Security Affairs**

---

**DISTRIBUTION:**  
All Departmental Elements

**INITIATED BY:**  
Office of Nuclear and  
National Security Information

## IDENTIFYING CLASSIFIED INFORMATION

1. **PURPOSE.** This Manual provides requirements for managing the Department of Energy (DOE) classification and declassification program, including details for classifying and declassifying information, documents, and material. This Manual also supplements DOE O 200.1, INFORMATION MANAGEMENT PROGRAM, which combines broad information management topics under a single Order. Specific requirements for each topic are issued in separate Manuals.
2. **CANCELLATION.** DOE M 475.1-1, IDENTIFYING CLASSIFIED INFORMATION, dated 5-8-98.
3. **APPLICABILITY.**
  - a. **DOE Elements.** This Manual applies to all DOE elements, including the National Nuclear Security Administration (NNSA), that may generate classified information, documents, or material.
  - b. **DOE Contractors.** The Contractor Requirements Document (CRD) sets forth requirements to be applied to DOE, NNSA, and DOE and NNSA contractors and subcontractors that may generate classified information, documents, or material. Contractor compliance with the CRD shall be required to the extent set forth in a contract.
4. **USAGE.** This Manual is divided into the following chapters:
  - a. **Chapter I - Responsibilities and Authorities.** Lists specific responsibilities and authorities for DOE Headquarters and field element officials and employees, including NNSA officials and employees.
  - b. **Chapter II - Program Administration.** Part A contains qualification and designation requirements for Classification Officers, Headquarters Classification Representatives, Original Classifiers, Derivative Classifiers, and Derivative Declassifiers. Part B contains administrative policies that apply to the overall classification and declassification program.
  - c. **Chapter III - Classification Categories and Levels.** Provides an overview of the categories of classified information and what levels may be applied to these categories.
  - d. **Chapter IV - Classifying and Declassifying Information.** Describes how information is initially classified, declassified, downgraded or upgraded, or reclassified. Requirements in this chapter are applied by the Director of Nuclear and National Security Information, the Director of Security Affairs, and Original Classifiers.

- e. Chapter V - Classification Guidance. Describes the classification guidance system, which specifies the information that is classified and unclassified.
  - f. Chapter VI - Classifying and Declassifying Documents and Material. Describes how documents and material are classified, declassified, downgraded or upgraded, or reclassified. Requirements in this chapter are applied by originators of documents and material, Derivative Classifiers, Derivative Declassifiers, Classification Officers, Headquarters Classification Representatives, the Director of Nuclear and National Security Information, and the Director of Security Affairs.
  - g. Chapter VII - Education Program. Describes training needed by Original and Derivative Classifiers, Derivative Declassifiers, and other DOE, including NNSA, cleared employees who generate classified information.
  - h. Chapter VIII - Classification and Declassification Oversight Program. Describes elements of the oversight program to ensure that organizations generating classified information, documents, and material maintain an adequate and effective classification and declassification program.
  - i. Contractor Requirements Document (Attachment 2) - Describes the requirements that apply to contractors.
5. DEFINITIONS. Definitions of terms used throughout this Manual can be found in Attachment 1.
6. CONTACT. Questions concerning this Manual should be addressed to the Policy and Quality Management Division, Office of Nuclear and National Security Information (301-903-5454).

BY ORDER OF THE SECRETARY OF ENERGY:



ARCHER L. DURHAM  
Assistant Secretary for  
Human Resources and Administration

## CONTENTS

### CHAPTER I—RESPONSIBILITIES AND AUTHORITIES

1.	Secretary .....	I-1
2.	Heads of Program and Support Offices within DOE, Including NNSA .....	I-1
3.	Director of Security Affairs .....	I-1
4.	Director of Nuclear and National Security Information .....	I-1
5.	Heads of DOE Elements, NNSA Deputy Administrators, and Managers of Field Elements .....	I-2
6.	Headquarters Classification Representatives .....	I-2
7.	Field Element Classification Officers .....	I-2
8.	Deputy Administrator for Naval Reactors .....	I-3
9.	Individuals Originating Procurement Requests .....	I-3
10.	Contracting Officers .....	I-3
11.	DOE Employees, including NNSA Employees, with Access Authorizations .....	I-3

### CHAPTER II—PROGRAM ADMINISTRATION

#### PART A—QUALIFICATIONS AND DESIGNATIONS .....

II-1

1.	Classification Officer .....	II-1
a.	Requirement for Position .....	II-1
b.	Qualifications .....	II-1
c.	Nomination .....	II-1
d.	Training Requirement .....	II-1
e.	Approval of Nominee .....	II-2
f.	Removal from Position .....	II-2
2.	Headquarters Classification Representative .....	II-2
a.	Requirement for Position .....	II-2
b.	Qualifications .....	II-2
c.	Nomination .....	II-2
d.	Training Requirement .....	II-2
e.	Approval of Nominee .....	II-3
f.	Removal from Position .....	II-3
3.	Original Classifier .....	II-3
a.	Designation by Secretary of Energy .....	II-3
b.	Designation by Director of Nuclear and National Security Information .....	II-3
4.	Derivative Classifier .....	II-6
a.	Qualifications .....	II-6
b.	Designation Process .....	II-6
c.	Duration of Authority .....	II-7
d.	Redelegation .....	II-7
e.	Cancellation of Authority .....	II-7

## CONTENTS (continued)

f.	Notification of Vacant Headquarters Position .....	II-9
5.	Derivative Declassifier .....	II-9
a.	Qualifications .....	II-9
b.	Designation Process .....	II-9
c.	Duration of Authority .....	II-10
d.	Redelegation .....	II-10
e.	Cancellation of Authority .....	II-10
f.	Notification of Vacant Position .....	II-11
<b>PART B - ADMINISTRATIVE POLICIES .....</b>		<b>II-12</b>
1.	Challenges to Classification .....	II-12
a.	Restricted Data/Formerly Restricted Data .....	II-12
b.	National Security Information .....	II-12
2.	Reporting Requirements .....	II-13
3.	Misclassification of Information, Documents, or Material .....	II-13
a.	Deliberate Action .....	II-13
b.	Negligence in Exercising Classification/Declassification Authority .....	II-13
4.	Deviations From Requirements .....	II-13
<b>CHAPTER III - CLASSIFICATION CATEGORIES AND LEVELS</b>		
1.	Categories of Classified Information .....	III-1
a.	Restricted Data and Formerly Restricted Data .....	III-1
b.	National Security Information .....	III-1
2.	Levels of Classification .....	III-1
a.	Top Secret .....	III-1
b.	Secret .....	III-1
c.	Confidential .....	III-1
3.	Use of the Term "Unclassified" .....	III-2
<b>CHAPTER IV - CLASSIFYING AND DECLASSIFYING INFORMATION</b>		
<b>PART A - RESTRICTED DATA .....</b>		<b>IV-1</b>
1.	Initial Classification .....	IV-1
a.	Authority .....	IV-1
b.	Classification Level Assignment .....	IV-1
c.	Request for Determination .....	IV-1
2.	Declassification .....	IV-1
a.	Authority .....	IV-1
b.	Unauthorized Disclosure .....	IV-1
c.	Declassification Proposals .....	IV-1

**CONTENTS (continued)**

3. Downgrading or Upgrading ..... IV-2  
4. Reclassification ..... IV-2  
5. Notification Requirements ..... IV-2

**PART B - FORMERLY RESTRICTED DATA ..... IV-3**

1. Transclassification ..... IV-3  
    a. Authority ..... IV-3  
    b. Classification Level Assignment ..... IV-3  
2. Declassification ..... IV-3  
    a. Authority ..... IV-3  
    b. Unauthorized Disclosure ..... IV-3  
    c. Declassification Proposals ..... IV-3  
3. Downgrading or Upgrading ..... IV-3  
4. Reclassification ..... IV-3  
5. Notification Requirements ..... IV-3

**PART C - NATIONAL SECURITY INFORMATION ..... IV-4**

1. Original Classification ..... IV-4  
    a. Original Classification Standards ..... IV-4  
    b. Classification Categories ..... IV-4  
    c. Classification Level Assignment ..... IV-5  
    d. Duration of Classification ..... IV-5  
    e. Extension of Classification ..... IV-6  
    f. Required Markings ..... IV-6  
    g. Reporting Original Determinations ..... IV-7  
2. Declassification ..... IV-7  
    a. Authority ..... IV-7  
    b. Unauthorized Disclosure ..... IV-7  
    c. Declassification Criteria ..... IV-7  
    d. Declassification Proposals ..... IV-7  
3. Downgrading or Upgrading ..... IV-7  
4. Reclassification ..... IV-8  
5. Notification Requirements ..... IV-8

**CHAPTER V - CLASSIFICATION GUIDANCE**

1. General ..... V-1  
    a. Purpose ..... V-1  
    b. Content ..... V-1  
    c. Inconsistent Guidance ..... V-1  
    d. No Guidance ..... V-1

**CONTENTS (continued)**

2.	Types of Guidance .....	V-2
a.	Headquarters Guidance .....	V-2
b.	Local Guidance .....	V-2
3.	Related Policies and Procedures .....	V-3
a.	Updating Guidance .....	V-3
b.	Classification Guidance for DOE, Including NNSA, Contractors .....	V-4
c.	Classification Guidance for Non-DOE, Including non-NNSA, Funded Work ...	V-4
d.	Classification Guidance for Jointly Funded Work .....	V-5
e.	Classification Guidance for DOE-Funded Work at Other Government Facilities (Including Work Funded by NNSA) .....	V-5

**CHAPTER VI - CLASSIFYING AND DECLASSIFYING DOCUMENTS AND MATERIAL****PART A - CLASSIFICATION .....** VI-1

1.	Authority .....	VI-1
a.	Restricted Data/Formerly Restricted Data .....	VI-1
b.	National Security Information .....	VI-1
2.	Review Requirements .....	VI-1
a.	Current Employee .....	VI-1
b.	Not an Employee .....	VI-2
3.	Required Markings .....	VI-3
a.	Restricted Data/Formerly Restricted Data .....	VI-3
b.	National Security Information .....	VI-3
c.	Mixed Document .....	VI-4
4.	Portion Marking Requirements .....	VI-4
a.	Restricted Data/Formerly Restricted Data Documents .....	VI-5
b.	National Security Information Documents .....	VI-5
c.	Mixed Documents .....	VI-5
d.	Documents Prepared Under Work-for-Others Contracts .....	VI-5
5.	Notification of Classification .....	VI-5
6.	Procedures Related to the Review of Documents or Material for Classification .....	VI-5
a.	Foreign Government Information .....	VI-5
b.	Use of a Classified Addendum .....	VI-5
c.	Review of Patent Applications and Reports .....	VI-6
d.	External Coordination Reviews .....	VI-6
e.	Classification Following Request for a Previously Unclassified Document .....	VI-6

**PART B - DECLASSIFICATION .....** VI-7

1.	Authority .....	VI-7
2.	Review Requirements for Redacting a Document or Declassifying a Document or Material .....	VI-7

**CONTENTS (continued)**

3.	Required Markings .....	VI-7
4.	Duration of Classification .....	VI-7
	a. Restricted Data/Formerly Restricted Data .....	VI-7
	b. National Security Information .....	VI-7
5.	Types of Document Reviews .....	VI-8
	a. Freedom of Information Act Requests .....	VI-8
	b. Privacy Act Requests .....	VI-9
	c. Mandatory Review Requests .....	VI-9
	d. Systematic Reviews .....	VI-10
	e. Other Reviews .....	VI-10
6.	Document Review Plan .....	VI-10
	a. Determining Need for a Plan .....	VI-10
	b. Contents of the Plan .....	VI-11
	c. Submission and Approval of the Plan .....	VI-11
7.	Notification of Declassification .....	VI-11
8.	Procedures Related to the Declassification Review of Documents or Material .....	VI-11
	a. Public Release .....	VI-11
	b. External Coordination Reviews .....	VI-11
	c. OpenNet Data Base .....	VI-12
	d. Obsolete Classification Markings .....	VI-12
	e. Extracted Version of Document .....	VI-13
	f. Redacted Version of Document .....	VI-13
	g. Review Upon Termination of Employment .....	VI-13
PART C - DOWNGRADING OR UPGRADING .....		VI-14
1.	General .....	VI-14
2.	Authority .....	VI-14
	a. Downgrading .....	VI-14
	b. Upgrading .....	VI-14
3.	Notification of Downgrading or Upgrading .....	VI-14
	a. Downgrading .....	VI-14
	b. Upgrading .....	VI-14
PART D - RECLASSIFICATION .....		VI-15
1.	Authority .....	VI-15
	a. General .....	VI-15
	b. Following Request for a Previously Declassified Document .....	VI-15
2.	Notification of Reclassification .....	VI-15

**CONTENTS (continued)****CHAPTER VII - EDUCATION PROGRAM**

1.	Initial Classification Education .....	VII-1
2.	Continuing Education .....	VII-1
3.	Initial Training for a Classifier or Declassifier .....	VII-1
	a. Original Classifier .....	VII-1
	b. Derivative Classifier .....	VII-1
	c. Derivative Declassifier .....	VII-2
4.	Recertification Training .....	VII-2

**CHAPTER VIII, CLASSIFICATION AND DECLASSIFICATION****OVERSIGHT PROGRAM**

1.	Performance Objective .....	VIII-1
2.	Scope .....	VIII-1
	a. Differing Scope and Complexity .....	VIII-1
	b. Uniformity of Oversight Reviews .....	VIII-1
3.	Frequency of Oversight Reviews .....	VIII-1
	a. Past Performance Experience and Review Results .....	VIII-1
	b. Interval Since Last Review .....	VIII-1
4.	Oversight Review Reports .....	VIII-2
5.	Follow-up Measures .....	VIII-2
6.	Self-Assessments .....	VIII-2

ATTACHMENT 1	DEFINITIONS .....	1-1
--------------	-------------------	-----

## CHAPTER I

### RESPONSIBILITIES AND AUTHORITIES

All responsibilities and authorities are limited to those within the cognizance or jurisdiction of the individual(s) indicated.

1. SECRETARY delegates Top Secret Original Classification Authority to those principal subordinates who require such authority. This authority may not be redelegated, but is assumed by an individual acting in a position with the authority.
2. HEADS OF PROGRAM AND SUPPORT OFFICES WITHIN DOE, INCLUDING NNSA, ensure that information, documents, and material are reviewed and processed in accordance with requirements in this Manual.
3. DIRECTOR OF SECURITY AFFAIRS.
  - a. Establishes DOE classification and declassification program requirements, including requirements for NNSA, under the Atomic Energy Act of 1954, as amended, and Executive Order 12958.
  - b. Declassifies and transclassifies Restricted Data (RD) and declassifies Formerly Restricted Data (FRD) under the Atomic Energy Act of 1954, as amended.
  - c. For DOE, including NNSA, makes the final appeal determination concerning the release of any portion of a document requested under statute or Executive order that was previously denied because it was classified.
4. DIRECTOR OF NUCLEAR AND NATIONAL SECURITY INFORMATION.
  - a. Develops, implements, and interprets DOE classification and declassification policy, regulations, and procedures, including policy, regulations, and procedures for NNSA.
  - b. Serves as the senior agency official responsible for directing and administering the DOE classification/declassification program under Executive Order 12958, including the program for NNSA, except for those provisions of the Executive order and implementing directives that deal with protecting classified information (e.g., personnel security, physical security, information security, and special access programs).
  - c. For DOE, including NNSA, manages programs for reviewing documents and material for classification, declassification, downgrading, upgrading, and reclassification.
  - d. For DOE, including NNSA, serves as the DOE Headquarters Classification Officer.

5. HEADS OF DOE ELEMENTS, NNSA DEPUTY ADMINISTRATORS, AND MANAGERS OF FIELD ELEMENTS.

- a. Ensure that the necessary staff are designated to fulfill the requirements contained in this Manual. (See Chapter II.)
- b. Ensure that information, documents, and material are reviewed and processed in accordance with the requirements in this Manual. (See Chapters IV and VI.)
- c. Ensure that Headquarters Classification Representatives, Classification Officers, and other personnel with classification responsibilities participate in the early planning stages of any new program that may generate classified information, documents, or material.
- d. Ensure that the management of classified information is included as a critical element or item to be evaluated in the performance standards of Headquarters Classification Representatives, Classification Officers, Original Classifiers, and any other individuals whose duties include significant involvement in generating classified information, documents, or material.
- e. Identify/appoint an individual to be responsible for notifying the contracting officer of each procurement falling within the scope of this Manual. If such an individual is not identified or appointed, the person originating the procurement request assumes this responsibility.

6. HEADQUARTERS CLASSIFICATION REPRESENTATIVES.

- a. Serve as the points of contact with the Office of Nuclear and National Security Information for their Headquarters elements.
- b. Coordinate the classification and declassification reviews of documents and material for their organizations.
- c. Assist individuals within their organizations in implementing the classification and declassification policies and procedures in this Manual; refer questions, as necessary, to the Office of Nuclear and National Security Information.

7. FIELD ELEMENT CLASSIFICATION OFFICERS.

- a. Serve as the points of contact with the Office of Nuclear and National Security Information for their field elements.
- b. Administer the field element classification and declassification programs.
- c. Ensure that a classification review is performed prior to the dissemination of each document that may be classified and that is prepared by a field element employee.

8. DEPUTY ADMINISTRATOR FOR NAVAL REACTORS implements and oversees all policy and practices pertaining to this Manual for activities under the Director's cognizance.
9. INDIVIDUALS ORIGINATING PROCUREMENT REQUESTS or such other individual(s) identified/appointed by the cognizant head of the DOE or NNSA element.
  - a. Bring to the attention of the cognizant contracting officer the following:
    - (1) each procurement requiring the inclusion of all or part of the CRD attached to this Order (reference 48 CFR Part 952.204-70) and
    - (2) flowdown requirements to any subcontract or subaward.
  - b. Identify the classification guidance that applies to each proposed contract or subcontract.
10. CONTRACTING OFFICERS, based on advice received from the person originating a procurement request or the individual identified/appointed by the head of the cognizant DOE, including NNSA, element, apply requirements contained in the CRD attached to this Manual to DOE and NNSA contractors.
11. DOE EMPLOYEES (INCLUDING NNSA EMPLOYEES) WITH ACCESS AUTHORIZATIONS.
  - a. Submit any potentially classified document or material they originate to a Derivative Classifier for classification review and a determination prior to dissemination outside of the employee's immediate organization.
  - b. Submit any potentially classified document or material they originate that is intended for widespread distribution or public release to the local Classification Officer for classification review and a determination prior to dissemination.
  - c. Ensure that any document or material that may be classified is determined to be unclassified and appropriate for public release before it is removed from official premises by an employee who is retiring or otherwise terminating employment.

## CHAPTER II

### PROGRAM ADMINISTRATION

#### PART A - QUALIFICATIONS AND DESIGNATIONS

##### 1. CLASSIFICATION OFFICER.

###### a. Requirement for Position.

- (1) Field Element. Each DOE field element, including NNSA field elements, that generate classified information must have a Classification Officer.
- (2) Contractor. The field element Classification Officer shall determine when a contractor under his/her cognizance is required to designate a Classification Officer.

b. Qualifications. A Classification Officer must have a scientific or technical degree related to the field in which he/she is working. The Director of Nuclear and National Security Information may waive this requirement for nominees with suitable experience. Each Classification Officer shall also be an Original and Derivative Classifier and a Derivative Declassifier.

###### c. Nomination.

- (1) Field Element. The head of a field element shall nominate an individual for the position of Classification Officer by submitting that individual's name and qualifications to the Director of Nuclear and National Security Information. For NNSA field elements, the nomination must be submitted through the Chief of Defense Nuclear Security.
- (2) Contractor. The head of each contractor organization shall nominate an individual for the position of Classification Officer by submitting that individual's name and qualifications to the field element Classification Officer for review. The field element Classification Officer shall submit the nomination to the Director of Nuclear and National Security Information with a recommendation for approval if the qualifications are adequate. For NNSA field elements, the nomination must be submitted through the Chief of Defense Nuclear Security. If the qualifications are not adequate, the field element Classification Officer shall return the nomination to the head of the contractor organization for reconsideration.

d. Training Requirement. In addition to meeting the qualifications specified above, each nominee must successfully complete the training course given by the Office of Nuclear and National Security Information.

- e. Approval of Nominee. The Director of Nuclear and National Security Information approves nominees to serve as Classification Officers. For NNSA field elements and contractor organizations, the Director of Nuclear and National Security Information provides the Chief of Defense Nuclear Security with a copy of the approval notification memorandum.
- f. Removal from Position. The head of the field element, the Chief of Defense Nuclear Security for NNSA field elements, or the Director of Nuclear and National Security Information may remove an employee from the Classification Officer position when the employee cannot or does not perform his/her responsibilities reliably.
- (1) Removal by the Head of the Field Element. The head of the field element shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA field elements) of the removal, the reason for removal, and the effective date.
  - (2) Removal by the Chief of Defense Nuclear Security. The Chief of Defense Nuclear Security shall notify the employee and inform the head of the NNSA field element and the Director of Nuclear and National Security Information of the removal, the reason for removal, and the effective date.
  - (3) Removal By the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information shall notify the employee and inform the head of the field element (as well as the Chief of Defense Nuclear Security for NNSA field elements) of the removal, the reason for removal, and the effective date.

## 2. HEADQUARTERS CLASSIFICATION REPRESENTATIVE.

- a. Requirement for Position. Each DOE Headquarters element, including NNSA Headquarters elements, that generate classified information must have a Headquarters Classification Representative.
- b. Qualifications. A Headquarters Classification Representative shall be a Derivative Classifier.
- c. Nomination. The head of a DOE Headquarters element, including NNSA Headquarters elements, shall nominate an individual for the position of Headquarters Classification Representative by submitting his/her name and qualifications to the Director of Nuclear and National Security Information. For NNSA Headquarters elements, the nomination must be sent through the Chief of Defense Nuclear Security.
- d. Training Requirement. In addition to meeting the qualifications specified above, each nominee must successfully complete the training course given by the Office of Nuclear and National Security Information.

- e. Approval of Nominee. The Director of Nuclear and National Security Information approves nominees to serve as Headquarters Classification Representatives. For NNSA Headquarters elements, the Director of Nuclear and National Security Information provides the Chief of Defense Nuclear Security with a copy of the approval notification memorandum.
- f. Removal from Position. The head of a DOE Headquarters element, including the heads of NNSA Headquarters elements, the Chief of Defense Nuclear Security for NNSA Headquarters elements, or the Director of Nuclear and National Security Information may remove an employee from the Headquarters Classification Representative position when the employee cannot or does not perform his/her responsibilities reliably.
  - (1) Removal by the Head of a DOE Headquarters Element, including the Heads of NNSA, Headquarters Elements. The head of a DOE Headquarters element, including NNSA Headquarters elements, shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA Headquarters elements) of the removal, the reason for removal, and the effective date.
  - (5) Removal by the Chief of Defense Nuclear Security. The Chief of Defense Nuclear Security shall notify the employee and inform the head of the NNSA Headquarters element and the Director of Nuclear and National Security Information of the removal, the reason for removal, and the effective date.
  - (3) By the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information shall notify the employee and inform the head of the DOE Headquarters element, including NNSA Headquarters elements (as well as the Chief of Defense Nuclear Security for NNSA Headquarters elements) of the removal, the reason for removal, and the effective date.

3. ORIGINAL CLASSIFIER.

- a. Designation by Secretary of Energy. The Secretary of Energy designates individuals occupying certain positions as Top Secret Original Classifiers. Such authority may not be re delegated, but is assumed by an individual acting in a position with the authority. (Individuals designated by the Secretary automatically have Secret and Confidential original classification authority and are not subject to the requirements in Paragraph b, below. In addition, such individuals are automatically granted derivative classification authority at the Top Secret, Secret, and Confidential levels.)
- b. Designation by Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information designates specific individuals as Secret or Confidential Original Classifiers. These individuals may exercise original classification authority only while occupying those positions for which the authority was granted. This

authority may not be assumed by an individual serving in an acting capacity. This authority is not retained when the individual transfers to another position. If an individual vacates a position that requires original classification authority, the individual who will permanently fill the vacancy is not automatically granted the authority, but is designated only in accordance with the procedures in Paragraph 3b(2) below.

- (1) Qualifications. To be nominated as an Original Classifier, an individual shall—
  - (a) be a Federal employee;
  - (b) have demonstrated competence in the subject area in which the authority will be used; and
  - (c) be familiar with DOE classification policy and procedures, especially in the subject area for which the authority will be used.
  
- (2) Designation Process.
  - (a) Request for Designation. The office director or higher authority shall submit a designation request to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA Headquarters and field elements). The Office of Nuclear and National Security Information (301-903-0368) can provide detailed instructions on how to submit the request.
  - (b) Evaluation of Request. The Director of Nuclear and National Security Information shall evaluate the need for the authority and the qualifications of the individual.
  - (c) Required Training.
    - 1 New Original Classifier. Prior to being designated as an Original Classifier, each employee shall successfully complete a training program and examination specified by the Office of Nuclear and National Security Information.
    - 2 Original Classifier Recertification. To recertify as an Original Classifier, an employee must successfully complete an examination given by the Office of Nuclear and National Security Information.
    - 3 Waiver of Required Training. The Director of Nuclear and National Security Information may waive the required training and examination for an employee who has met the requirements

within the last 3 years and who is transferring from a similar programmatic position.

- (d) Designation. The Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements) shall designate in writing each Secret or Confidential Original Classifier. Each designation shall describe the specific subject areas covered by the Original Classifier's authority and state the date the authority expires.
- (3) Duration of Authority. Original classification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.
- (4) Redelegation. Authority granted under this chapter, Part A, Paragraph 3b, cannot be redelegated.
- (5) Cancellation of Authority. The office director, the Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel original classification authority when an employee's position no longer requires such authority or an employee occupying a position with original classification authority cannot or does not exercise that authority reliably.
  - (a) By the Office Director. The office director who cancels the original classification authority for an employee shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date when the authority will end.
  - (b) By the Chief of Defense Nuclear Security. Upon canceling the original classification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the employee's office director and the Director of Nuclear and National Security Information, providing the employee's name and position, the reason for cancellation, and the date when the authority will end.
  - (c) By the Director of Nuclear and National Security Information. Upon canceling the original classification authority for an employee, the Director of Nuclear and National Security Information shall notify the employee and inform the employee's office director (as well as the Chief of Defense Nuclear Security for NNSA elements), providing the employee's name and position, the reason for cancellation, and the date when the authority will end.

- (6) Notification of Vacant Position. When an employee vacates a position that requires original classification authority, the Headquarters Classification Representative or the field element Classification Officer shall promptly inform the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements) of the employee's name, position, and date of departure.
4. DERIVATIVE CLASSIFIER. Classification Officers designate specific individuals as Derivative Classifiers. These individuals may exercise derivative classification authority only while occupying those positions for which the authority was granted. This authority may not be assumed by an individual serving in an acting capacity. This authority is not retained when the individual transfers to another position. If an individual vacates a position that requires derivative classification authority, the individual who will permanently fill the vacancy is not automatically granted the authority, but is designated only in accordance with the procedures in Paragraph 4b below.
- a. Qualifications. To be nominated as a Derivative Classifier, an employee shall—
    - (1) have demonstrated competence in the subject area in which the authority will be used and
    - (2) be familiar with DOE classification policy, procedures, and guidance, especially in the subject area for which the authority will be used.
  - b. Designation Process.
    - (1) Designating Official.
      - (a) Top Secret Derivative Classifiers. The Director of Nuclear and National Security Information designates all Top Secret Derivative Classifiers. (For NNSA elements, the Director of Nuclear and National Security Information provides the Chief of Defense Nuclear Security with a copy of the written designation.)
      - (b) Secret and Confidential Derivative Classifiers. The local Classification Officer designates Secret and Confidential Derivative Classifiers for organizations under his/her purview and shall maintain a current list of such designations.
    - (2) Request for Designation. The office director or higher authority shall submit a designation request to the designating official following instructions issued by the local classification office.
    - (3) Evaluation of Request. The designating official shall evaluate the need for the authority and the qualifications of the individual.

- (4) Required Training.
  - (a) New Derivative Classifier. Prior to being designated as a Derivative Classifier, each employee shall successfully complete a training program and examination specified by the designating official.
  - (b) Derivative Classifier Recertification. To recertify as a Derivative Classifier, an employee shall successfully complete an examination specified by the designating official.
  - (c) Waiver of Required Training. The designating official may waive the required training and examination for an employee who has met the requirements within the last 3 years and who is transferring from a similar programmatic position.
- (5) Designation. The designating official shall designate in writing each Derivative Classifier. Each designation shall describe the specific subject areas covered by the Derivative Classifier's authority and state the date the authority expires.
  - c. Duration of Authority. Derivative classification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.
  - d. Redelegation. Derivative classification authority cannot be redelegated.
  - e. Cancellation of Authority.
    - (1) Top Secret. The office director, the Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel Top Secret derivative classification authority when the employee's position no longer requires such authority or the employee cannot or does not exercise that authority reliably.
      - (a) By the Office Director. The office director who cancels the Top Secret derivative classification authority for an employee shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date the authority will end.
      - (b) By the Chief of Defense Nuclear Security. Upon canceling the Top Secret derivative classification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the office director and the Director of Nuclear and National Security Information of the employee's name and position, the reason for cancellation, and the date the authority will end.

- (c) By the Director of Nuclear and National Security Information. Upon canceling the Top Secret derivative classification authority for an employee, the Director of Nuclear and National Security Information shall notify the employee and inform the office director (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (2) Secret and Confidential. The office director, the designating official, the Field Element Classification Officer for contractors under his/her cognizance, the Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel Secret or Confidential derivative classification authority when the employee's position no longer requires such authority or the employee cannot or does not exercise that authority reliably.
- (a) By the Office Director. The office director who cancels the Secret or Confidential derivative classification authority for an employee shall notify the employee and inform the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (b) By the Designating Official. The designating official who cancels the Secret or Confidential derivative classification authority for an employee shall notify the employee and inform the employee's office director of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (c) By the Field Element Classification Officer. The Field Element Classification Officer who cancels the Secret or Confidential derivative classification authority for a contractor employee under his/her cognizance shall notify the employee and inform the employee's office director and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (c) By the Chief of Defense Nuclear Security. Upon canceling the Secret or Confidential derivative classification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the employee's office director and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (d) By the Director of Nuclear and National Security Information. Upon canceling the Secret or Confidential derivative classification authority for an employee, the Director of Nuclear and National Security

Information shall notify the employee and inform the employee's office director and the designating official (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date the authority will end.

- f. Notification of Vacant Headquarters Position. When a Headquarters employee vacates a position that requires derivative classification authority, the Headquarters Classification Representative shall promptly inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA Headquarters elements) of the employee's name, position, and date of departure.
5. DERIVATIVE DECLASSIFIER. The Director of Nuclear and National Security Information designates specific individuals as Derivative Declassifiers. These individuals may exercise derivative declassification authority only while occupying those positions for which the authority was granted. This authority may not be assumed by an individual serving in an acting capacity. This authority is not retained when the individual transfers to another position. If an individual vacates a position that requires derivative declassification authority, the individual who will permanently fill the vacancy is not automatically granted the authority, but is designated only in accordance with the procedures in Paragraph 5b below.
- a. Qualifications. To be nominated as a Derivative Declassifier, an employee shall—
    - (1) have a scientific or technical degree (the Director of Nuclear and National Security Information may waive this requirement for nominees with suitable experience);
    - (2) have demonstrated competence in the subject area in which the authority will be used; and
    - (3) be familiar with DOE classification and declassification policy, procedures, and guidance, especially in the subject area for which the authority will be used.
  - b. Designation Process.
    - (1) Request for Designation. The office director or higher authority shall submit a designation request to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements). The Office of Nuclear and National Security Information (301-903-0368) can provide detailed instructions on how to submit the request.
    - (2) Evaluation of Request. The Director of Nuclear and National Security Information shall evaluate the need for the authority and the qualifications of the individual.

- (3) Required Training.
- (a) New Derivative Declassifier. Prior to being designated as a Derivative Declassifier, each employee shall successfully complete a training program and examination given by the Office of Nuclear and National Security Information. In addition, the local classification office shall provide training specific to the documents and material being reviewed for declassification.
  - (b) Derivative Declassifier Recertification. To recertify as a Derivative Declassifier, an employee shall successfully complete an examination given by the Office of Nuclear and National Security Information.
  - (c) Waiver of Required Training. The Director of Nuclear and National Security Information may waive the required training and examination for an employee who has met the requirements within the last 3 years and who is transferring from a similar programmatic position.
- (4) Designation. The Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements) shall designate in writing each Derivative Declassifier. Each designation shall identify the organizations and specific subject areas covered by the Derivative Declassifier's authority and state the date the authority expires.
- c. Duration of Authority. Derivative declassification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.
  - d. Redelegation. Derivative declassification authority cannot be redelegated.
  - e. Cancellation of Authority. The office director, Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel derivative declassification authority when an employee's position no longer requires such authority or the employee cannot or does not exercise that authority reliably.
    - (1) By Office Director. The office director who cancels the derivative declassification authority for an employee shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date the authority will end.
    - (2) By the Chief of Defense Nuclear Security. Upon canceling the derivative declassification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the office director and the

Director of Nuclear and National Security Information of the employee's name and position, the reason for cancellation, and the date the authority will end.

- (2) By Director of Nuclear and National Security Information. Upon canceling the derivative declassification authority for an employee, the Director of Nuclear and National Security Information shall notify the employee and inform the office director (as well as the Chief of Defense Nuclear Security for NNSA elements) of the employee's name and position, the reason for cancellation, and the date the authority will end.

- f. Notification of Vacant Position. When an employee vacates a position that requires derivative declassification authority, the Headquarters Classification Representative or the field element Classification Officer shall promptly inform the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements) of the employee's name, position, and date of departure.

**PART B - ADMINISTRATIVE POLICIES****1. CHALLENGES TO CLASSIFICATION.****a. Restricted Data/Formerly Restricted Data.**

- (1) **Challenge.** An employee may formally challenge an RD/FRD classification determination with the Derivative Classifier who made the determination. Under no circumstances shall an individual be subject to retribution for such a challenge. The Derivative Classifier shall respond to the challenge within 90 calendar days. If no response is received, the employee may submit an initial appeal to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements).
- (2) **Initial Appeal to Director of Nuclear and National Security Information.** If the response by the Derivative Classifier does not satisfy the employee making the challenge, the employee may appeal the determination by writing to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements). The Director of Nuclear and National Security Information shall respond (with a copy to the Chief of Defense Nuclear Security for NNSA elements) within 90 calendar days. If no response is received, the employee may submit a final appeal to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA elements).
- (3) **Final Appeal to Director of Security Affairs.** If the response by the Director of Nuclear and National Security Information does not satisfy the employee making the challenge, the employee may appeal the determination to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA elements).

**b. National Security Information.**

- (1) **Challenge.** An employee may formally challenge an NSI classification determination by writing to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements). The Director of Nuclear and National Security Information shall respond (with a copy to the Chief of Defense Nuclear Security for NNSA elements) within 60 calendar days. Under no circumstances shall an individual be subject to retribution for such a challenge. If the Director is unable to respond within 60 calendar days, he/she shall acknowledge the challenge in writing and provide a date when the employee can expect a response. If the Director of Nuclear and National Security Information has not responded to the challenge within 120 calendar days, the employee may forward the challenge to

the Interagency Security Classification Appeals Panel (ISCAP), as described in Appendix A to 32 CFR Part 2001.

- (2) Appeal to Director of Security Affairs. If the response by the Director of Nuclear and National Security Information does not satisfy the employee making the challenge, the employee may appeal the determination to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA elements). The Director of Security Affairs shall respond (with a copy to the Chief of Defense Nuclear Security for NNSA elements) within 90 calendar days. If the Director of Security Affairs has not responded to the appeal within 90 calendar days, the employee may forward the challenge to the ISCAP, as described in Appendix A to 32 CFR Part 2001.
2. REPORTING REQUIREMENTS. Each Headquarters Classification Representative and field element Classification Officer shall compile statistics requested by the Office of Nuclear and National Security Information and provide them to the Director of Nuclear and National Security Information, with a copy to the Chief of Defense Nuclear Security for NNSA elements, for use in assessing DOE's, including NNSA's, success at meeting performance measurements and for inclusion in reports required by the Information Security Oversight Office and 10 CFR Part 1045.
3. MISCLASSIFICATION OF INFORMATION, DOCUMENTS, OR MATERIAL.
  - a. Deliberate Action. Any knowing or willful action that results in the misclassification of information, documents, or material violates the requirements in this Manual and may result in criminal, civil, and/or administrative penalties. Such an action may also result in a security infraction or violation, as covered under DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, and DOE O 471.2A, INFORMATION SECURITY PROGRAM. However, security infractions are not intended to be issued in cases where classifiers disagree for legitimate reasons. Examples of situations in which security infractions will be issued include classifying with no authority and classifying outside of granted authority.
  - b. Negligence in Exercising Classification/Declassification Authority. The appropriate official (as indicated in Part A of this chapter) shall promptly cancel the classification authority of any individual who demonstrates gross negligence or a pattern of negligence or carelessness in applying the requirements in this Manual that results in the misclassification of information, documents, or material.
4. DEVIATIONS FROM REQUIREMENTS. A Headquarters Classification Representative or Classification Officer may propose an alternate or equivalent means of meeting a specific requirement in this Manual or he/she may request an exemption. Such a proposal shall describe the variance or waiver and explain why it is needed. The proposal shall be submitted to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements) for approval within 30 days. Each approved deviation shall be examined during an oversight review to ensure it is still needed.

## CHAPTER III

### CLASSIFICATION CATEGORIES AND LEVELS

#### 1. CATEGORIES OF CLASSIFIED INFORMATION.

##### a. Restricted Data and Formerly Restricted Data.

(1) Restricted Data. Information classified under the Atomic Energy Act that concerns—

(a) the design, manufacture, or utilization of nuclear weapons;

(b) the production of special nuclear material; or

(c) the use of special nuclear material in the production of energy.

RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.

(2) Formerly Restricted Data. Information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.

b. National Security Information. Information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

#### 2. LEVELS OF CLASSIFICATION. The following levels of classification, listed in descending order of sensitivity, may be applied to RD, FRD, or NSI:

a. Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.

b. Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.

c. Confidential. The damage tests for RD/FRD and NSI are different, as noted below:

- (1) Restricted Data/Formerly Restricted Data. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - (2) National Security Information. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.
3. USE OF THE TERM "UNCLASSIFIED." The term "Unclassified" is used to identify information that is not classified under a statute or Executive order. Unclassified information is not normally marked as "Unclassified" except to distinguish it from classified information and then only when such distinction is required or otherwise serves a useful purpose. The fact that information is unclassified does not mean that it may be released to the public.

## CHAPTER IV

### CLASSIFYING AND DECLASSIFYING INFORMATION

#### PART A - RESTRICTED DATA

##### 1. INITIAL CLASSIFICATION.

- a. Authority. The Director of Nuclear and National Security Information initially determines whether nuclear-related information is RD under the Atomic Energy Act of 1954, as amended.
- b. Classification Level Assignment. The Director of Nuclear and National Security Information shall assign a classification level that reflects the sensitivity of the information to the common defense and security. The classification level assigned to the information is proportional to the risk to the common defense and security by unauthorized disclosure. (See Chapter III, Paragraph 2.)
- c. Request for Determination. An employee who develops a new, nuclear-related subject area that he/she believes may be classified shall request an evaluation of the subject area by the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements). The Director of Nuclear and National Security Information shall make a determination within 90 calendar days.

##### 2. DECLASSIFICATION.

- a. Authority. The Director of Nuclear and National Security Information shall continuously review RD information and recommend to the Director of Security Affairs all actions to remove information from that category.
- b. Unauthorized Disclosure. Information classified as RD is **not** declassified automatically because of any unauthorized disclosure of identical or similar information.
- c. Declassification Proposals. The Director of Security Affairs shall consider proposals from Federal and contractor employees of DOE, including NNSA, as well as proposals from the public and other agencies for declassifying RD information.
  - (1) Ad Hoc Proposals. At any time, Federal and contractor employees of DOE, including NNSA, may submit to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements) proposals for declassifying RD information. Such proposals may be submitted to achieve a variety of goals, such as challenging classification policy, reducing operating costs, or transferring technology to the private sector.

- (2) Call for Proposals. The Director of Nuclear and National Security Information shall periodically issue a call to DOE elements, including NNSA elements, as well as to the Department of Defense, for declassification proposals.
  - (3) Disposition of Proposal. Within 1 month after the final determination is made, the Director of Nuclear and National Security Information shall notify, through the Headquarters Classification Representative or field element Classification Officer (as well as through the Chief of Defense Nuclear Security for NNSA elements), each person or organization making a proposal of that proposal's final disposition.
3. DOWNGRADING OR UPGRADING. The Director of Nuclear and National Security Information may downgrade or upgrade the classification level of RD information.
  4. RECLASSIFICATION. Information once classified as RD but declassified cannot be reclassified. However, the Director of Nuclear and National Security Information may evaluate new information in a previously declassified subject area and then classify it, if warranted.
  5. NOTIFICATION REQUIREMENTS. The Director of Nuclear and National Security Information shall notify classifiers and declassifiers when information is classified, declassified, downgraded, or upgraded by issuing classification guidance.

## PART B - FORMERLY RESTRICTED DATA

1. TRANSCLASSIFICATION.
  - a. Authority. Certain RD information that relates primarily to the military utilization of nuclear weapons may be removed from the RD category and transclassified to FRD. This transclassification requires a joint determination between the Director of Security Affairs and appropriate officials within the Department of Defense.
  - b. Classification Level Assignment. At the time of transclassification, the Director of Security Affairs and appropriate officials from the Department of Defense shall assign a classification level that reflects the sensitivity of the information to the national security. The classification level assigned to the information is proportional to the risk to the common defense and security by unauthorized disclosure. (See Chapter III, Paragraph 2.)
2. DECLASSIFICATION.
  - a. Authority. The Director of Nuclear and National Security Information shall continuously review FRD information and recommend to the Director of Security Affairs all actions to remove information from that category. The decision to remove information from the FRD category is made in coordination with the Department of Defense.
  - b. Unauthorized Disclosure. Information classified as FRD is not declassified automatically because of any unauthorized disclosure of identical or similar information.
  - c. Declassification Proposals. The Director of Security Affairs shall consider proposals from Federal and contractor employees of DOE, including NNSA, as well as from the public and other agencies for declassifying FRD information. The process described in Part A, Paragraphs 2c(1)-(3) of this chapter, also applies to proposals for declassifying FRD information.
3. DOWNGRADING OR UPGRADING. The Director of Nuclear and National Security Information, in coordination with the Department of Defense, may downgrade or upgrade the classification level of FRD information.
4. RECLASSIFICATION. Information once classified as FRD but declassified cannot be reclassified. However, the Director of Nuclear and National Security Information, in coordination with the Department of Defense, may evaluate newly generated specific information in a previously declassified subject area and then classify it, if warranted.
5. NOTIFICATION REQUIREMENTS. The Director of Nuclear and National Security Information shall notify classifiers and declassifiers when information is classified, declassified, downgraded, or upgraded by issuing classification guidance.

**PART C - NATIONAL SECURITY INFORMATION**

1. **ORIGINAL CLASSIFICATION.** Under Executive Order 12958, an Original Classifier may determine that certain new information requires protection against unauthorized disclosure in the interest of national security. The Director of Nuclear and National Security Information may originally classify NSI in any subject area under DOE's, including NNSA's, cognizance at any level whenever classification guidance does not exist. An Original Classifier may originally classify NSI within his/her programmatic jurisdiction at any classification level up to and including the level (Top Secret, Secret, Confidential) of the Original Classifier's authority whenever classification guidance or relevant classified source documents do not exist.
  - a. **Original Classification Standards.**
    - (1) **Conditions for Classification.** Information may be originally classified as NSI only if all of the following conditions are met:
      - (a) An Original Classifier is classifying the information.
      - (b) The information is owned by, produced by or for, or is under the control of the U.S. Government.
      - (c) The information falls within one or more of the categories of information listed in Paragraph 1b below.
      - (d) An Original Classifier determines that the unauthorized disclosure of the information could reasonably be expected to result in damage to the national security that the Original Classifier can identify or describe.
    - (2) **Doubt about Classifying.** If significant doubt about the need to classify information exists, the information is not classified.
  - b. **Classification Categories.** Information may not be considered for classification unless it concerns—
    - (1) military plans, weapons systems, or operations;
    - (2) foreign government information;
    - (3) intelligence activities (including special activities), intelligence sources or methods, or cryptography;
    - (4) foreign relations or foreign activities of the United States, including confidential sources;
    - (5) scientific, technological, or economic matters relating to the national security;

- (6) U.S. Government programs for protecting and safeguarding nuclear materials or facilities; or
  - (7) vulnerabilities or capabilities of systems, installations, projects, or plans related to the national security.
- c. Classification Level Assignment. An Original Classifier shall assign a classification level that reflects the sensitivity of the information to the national security. The classification level assigned to the information is proportional to the risk to the national security by unauthorized disclosure. (See Chapter III, Paragraph 2.) If there is significant doubt about the appropriate level of classification, the information is classified at the lower level.
- d. Duration of Classification. Information may be classified for a period not to exceed 10 years unless it qualifies for an exemption from declassification.
- (1) Establishing Date or Event. At the time of original classification, an Original Classifier shall attempt to establish a specific date or event for declassification based on the national security sensitivity of the information, which shall not exceed 10 years unless he/she determines that the information meets one of the exemption criteria listed in Paragraph (3) below.
  - (2) Declassification in 10 Years. If the Original Classifier cannot establish a specific date or event for declassification, the information shall be marked for declassification 10 years from the date of the original decision, unless the information meets one of the exemption criteria listed in Paragraph (3) below.
  - (3) Exemption from Declassification. Information can be exempt from declassification only if an Original Classifier determines that the release of such information could reasonably be expected to—
    - (a) reveal an intelligence source, method, or activity, or a cryptographic system or activity;
    - (b) reveal information that would assist in the development or use of weapons of mass destruction;
    - (c) reveal information that would impair the development or use of technology within a United States weapons system;
    - (d) reveal United States military plans or national security emergency preparedness plans;
    - (e) reveal foreign government information;

- (f) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years;
  - (g) impair the ability of responsible U.S. Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
  - (h) violate a statute, treaty, or international agreement.
- e. Extension of Classification. An Original Classifier may extend the duration of classification for successive periods not to exceed 10 years at a time if such information continues to meet the standards for classification. (NOTE: This authority does not apply to information contained in documents that are more than 25 years old and determined to be permanent records under Title 44 of the United States Code.)
- f. Required Markings. The Original Classifier shall ensure the following markings are included on the document or material being originally classified (see DOE M 471.2-1A, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL, for complete information on marking requirements):
  - (1) Overall classification level of the document.
  - (2) Classification level of each interior page of the document if not using the overall classification level on each page.
  - (3) Portion marking for each section, part, paragraph, graphic, figure, or similar portion.
  - (4) Classification Authority (i.e., "Classified By").
    - (a) Name or personal identifier of the Original Classifier.
    - (b) Position title of the Original Classifier.
  - (5) NSI classification category identified in Paragraph 1b above (i.e., "Reason:").
  - (6) Duration of classification (i.e., "Declassify On")
    - (a) Date - A specific date 10 years or less from the date of the original decision.
    - (b) Event - A specific event occurring in less than 10 years.

- (c) Exempt from declassification - The information is exempt from declassification at 10 years based on criteria identified in Paragraph 1d(3) above.
  - (d) Extension of classification - Classification of the information may be extended for successive periods not to exceed 10 years at a time. The "Declassify On" line shall be revised to include the date of the extension action, the new declassification date, and the identity of the person authorizing the extension.
  - (e) Reclassification - Information may be reclassified for successive periods not to exceed 10 years at a time. The "Declassify On" line shall be revised to include the date of the reclassification, the new declassification date, and the identity of the person authorizing the reclassification.
- g. Reporting Original Determinations. An Original Classifier shall report each original classification determination to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements) within 10 working days of the determination. The report shall describe the information originally classified, identify the reason for classification, indicate the level and duration of classification, and identify the document, if any, containing the originally classified information. The originator of the report shall review it for classification; if the report is not classified or otherwise controlled, it shall be marked "Official Use Only" under Exemptions 2 and 5 of the Freedom of Information Act.

## 2. DECLASSIFICATION.

- a. Authority. The Director of Nuclear and National Security Information may declassify NSI in any subject area under DOE's, including NNSA's, cognizance. This authority may not be redelegated, but is assumed by an individual acting in that position.
- b. Unauthorized Disclosure. Information classified as NSI is not declassified automatically because of any unauthorized disclosure of identical or similar information.
- c. Declassification Criteria. NSI shall be declassified when it no longer meets the standards listed in Part C of this chapter, Paragraphs 1a and b.
- d. Declassification Proposals. The Director of Nuclear and National Security Information shall consider proposals from Federal and contractor employees of DOE, including NNSA, for declassifying NSI. The process described in Part A, Paragraphs 2c(1)-(3) of this chapter, also applies to proposals for declassifying NSI.

## 3. DOWNGRADING OR UPGRADING. The Director of Nuclear and National Security Information may downgrade or upgrade the classification level of NSI.

4. RECLASSIFICATION. NSI that has been formally declassified by proper authority may be reclassified only by the Director of Nuclear and National Security Information and only if it has not been released to the public.
5. NOTIFICATION REQUIREMENTS. The Director of Nuclear and National Security Information shall notify classifiers and declassifiers when information is classified, declassified, downgraded, upgraded, or reclassified by issuing instructions in classification guidance.

## CHAPTER V

### CLASSIFICATION GUIDANCE

#### 1. GENERAL.

- a. Purpose. Classification guidance contains detailed instructions for determining whether specific information is classified or unclassified. Examples of guidance include—but are not limited to—program guides, topical guides, local guides, bulletins, and change notices.
- b. Content. At a minimum, classification guidance identifies elements of information that are classified or unclassified in a specific area. For classified information, the guidance prescribes the classification level and category. For information classified as NSI, the guidance also states a concise reason for classifying the information and prescribes declassification instructions or the category for exemption from automatic declassification for each element of information.
- c. Inconsistent Guidance. Guidance may be inconsistent for three reasons; each reason requires a different course of action.
  - (1) Ambiguous Guidance. When information is described equally well by more than one topic but uncertainty exists about which topic applies, the most restrictive guidance shall apply until clarification is obtained.
  - (2) Outdated Guidance. Due to difficulties in revising all guidance simultaneously to reflect declassification actions, some guidance may specify different classifications for the same information. The guidance with the most current date shall apply.
  - (3) Conflicting Guidance. When the same information is classified differently in separate guidance and neither appears to be more current or authoritative than the other, the most restrictive guidance shall apply until clarification is obtained.
- d. No Guidance. A Derivative Classifier or Derivative Declassifier who cannot determine the proper classification of an element of information using classification guidance approved for his/her use shall contact the local Classification Officer for assistance. Local Classification Officers who cannot provide assistance shall refer the issue to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA elements). The Director of Nuclear and National Security Information shall make a classification determination within 90 calendar days. Pending this final determination, the document or material containing the information in question shall be marked and protected according to DOE M 471.2-1B, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL, issued by the Office of Safeguards and Security.

## 2. TYPES OF GUIDANCE.

### a. Headquarters Guidance.

- (1) Purpose. Headquarters guidance contains detailed classification and declassification instructions in one or more subject areas.
- (2) Originator/Approval Authority. Headquarters guidance covering only DOE, including NNSA, information is developed, approved, and issued by the Director of Nuclear and National Security Information. Headquarters guidance covering information for which DOE, including NNSA, and other Government agencies or foreign countries are responsible (known as joint guidance) is approved and issued by the Director of Nuclear and National Security Information in coordination with officials from the other Government agencies or foreign countries involved. Headquarters guidance shall name its approving official(s) and indicate the approval date.
- (3) Basis. Headquarters guidance is based on classification and declassification determinations made by the Directors of Nuclear and National Security Information and Security Affairs.
- (4) Users. Derivative Classifiers and Derivative Declassifiers use Headquarters guidance as the basis for derivative determinations; however, they may use only that guidance pertaining to the specific subject areas described in their designations of authority. A local classification office may also use Headquarters guidance to prepare detailed local guidance intended primarily for use within the field element or contractor organization.

### b. Local Guidance.

- (1) Purpose. Local guidance has the same purpose as Headquarters guidance, but is more detailed and is tailored to the specific needs of the originating field element or contractor organization. If existing Headquarters guidance is adequate for the needs of the organization, local guidance is not required. If proposed local guidance affects DOE, including NNSA, elements other than the issuing organization, a Government agency other than DOE (such as the Department of Defense), or a foreign government, the Director of Nuclear and National Security Information shall issue Headquarters guidance to cover the information.
- (2) Originator/Approval Authority. The local classification office may issue local guidance following approval by the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information may delegate approval authority in writing to field element Classification Officers on

a case-by-case basis. Local guidance shall name its approving official and indicate the approval date.

- (3) Basis. Local guidance is based on Headquarters guidance.
- (4) Users. Derivative Classifiers and Derivative Declassifiers shall use local guidance as the basis for derivative determinations; however, they may use only that guidance pertaining to the specific subject areas described in their designations of authority. Unless otherwise directed by the Director of Nuclear and National Security Information, local guidance may be disseminated to other organizations, both inside and outside DOE, providing each organization has a need to know and facility clearance at the appropriate classification level.
- (5) Copies of the Local Guidance. Within 10 calendar days of approval, any organization that issues local guidance shall send a disk containing the entire text of the guidance in either ASCII or WordPerfect (version 5.1 or higher) format and five copies of the issued guidance to the Director, Technical Guidance Division, Office of Nuclear and National Security Information.

### 3. RELATED POLICIES AND PROCEDURES.

#### a. Updating Guidance.

- (1) Erroneous Guidance. An issuing organization that learns its guidance contradicts current policy shall distribute revised guidance within 120 calendar days.
- (2) Periodic Review of Classification Guidance. Each organization that issues guidance shall maintain a list of its guidance and shall review and update such guidance as changes in classification policy are received (or in any event, at least once every 5 years) to ensure consistency with DOE classification policy. If the guidance is consistent with policy, the reviewer shall annotate the record copy of the guidance with the results and date of the review. If the guidance contradicts policy, the issuing organization shall revise the guidance and distribute it within 120 calendar days. Completion of this review does not require a specific report to the Director of Nuclear and National Security Information, but oversight reviews shall include an examination of these records of guidance review.
- (3) Distributing New or Revised Headquarters Guidance. Each Classification Officer shall distribute new or revised Headquarters guidance to appropriate classifiers and declassifiers within 30 calendar days of receiving it. However, if the new or revised Headquarters guidance affects local guidance, the Classification Officer shall revise and distribute the local guidance within 120 calendar days.

- b. Classification Guidance for DOE, including NNSA, Contractors.
- (1) Identification of Required Classification Guidance. Each individual originating a procurement request determines if a proposed contract may generate classified information. If it does, the procurement request originator shall complete Block 10 on DOE Form 5634.2, "Contract Security Classification Specification," which identifies classification guidance that will apply to the proposed contract. If necessary, the procurement request originator may request assistance from the cognizant classification office to identify the appropriate classification guidance.
  - (2) Approval of Classification Guidance. The appropriate classification official shall certify that the classification guidance identified in Block 10 is appropriate for the work to be performed.
    - (a) Headquarters Classification Representative. The Headquarters Classification Representative shall sign Block 15 of DOE Form 5634.2 for Headquarters-initiated procurements under his/her cognizance. This authority may be delegated in writing to specific Derivative Classifiers in the Representative's organization.
    - (b) Classification Officer. The Classification Officer shall sign Block 15 of DOE Form 5634.2 for field element-initiated procurements. This authority may be delegated in writing to specific Derivative Classifiers in the Classification Officer's organization. With the concurrence of the Director of Nuclear and National Security Information, the Classification Officer may also delegate this authority to a technically competent Derivative Classifier outside his/her staff.
- c. Classification Guidance for Non-DOE, including non-NNSA, Funded Work. Non-DOE, including non-NNSA, funded work that may generate classified information is conducted in accordance with DOE O 481.1, WORK FOR OTHERS (NON-DOE FUNDED WORK), and classification guidance is issued by the funding organization. For unclassified work, the funding organization shall provide a written statement that classified activities are not part of the project.
- (1) Certification of Guidance. The Classification Officer under whose purview the work will be conducted shall review the work request and the proposed classification guidance. He/she shall use DOE Form 5634.2, Department of Defense Form DD-254, "Contract Security Classification Specification," or any other form provided by the funding organization to certify that the guidance is adequate and does not contradict DOE policy. The Classification Officer may delegate the authority to review and certify classification guidance to a member of his/her staff. With the concurrence of the Director of Nuclear and National

Security Information, the Classification Officer may also delegate this authority to a technically competent Derivative Classifier outside his/her staff.

- (2) Additional Guidance Required. If additional guidance is required, DOE, including NNSA, the sponsoring agency, or both may develop the guidance, and the sponsoring agency shall approve it.
- d. Classification Guidance for Jointly Funded Work. Classification guidance for work conducted at DOE, including NNSA, facilities and funded by both DOE, including NNSA, and another U.S. Government organization is the joint responsibility of both funding organizations. The DOE, including NNSA, element responsible for the work shall contact the Office of Nuclear and National Security Information, through the Chief of Defense Nuclear Security for NNSA elements, to ensure that appropriate joint classification guidance is developed.
- e. Classification Guidance for DOE-Funded Work at Other Government Facilities (including work funded by NNSA). DOE, including NNSA, is responsible for issuing classification guidance for DOE, including NNSA, funded work at other Government facilities. The element responsible for the work shall contact the Office of Nuclear and National Security Information, through the Chief of Defense Nuclear Security for NNSA elements, to ensure that appropriate guidance is either available or developed.

## CHAPTER VI

### CLASSIFYING AND DECLASSIFYING DOCUMENTS AND MATERIAL

#### PART A - CLASSIFICATION

Secretarial Officers and heads of DOE, including NNSA, Headquarters and field elements shall ensure that documents and material prepared under their purview are reviewed and processed in accordance with the provisions of this part.

1. **AUTHORITY.** A Derivative Classifier may derivatively classify a document or material containing RD, FRD, and/or NSI only within his/her programmatic jurisdiction at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority.
  - a. **Restricted Data/Formerly Restricted Data.** A Derivative Classifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the classifier's designation of authority. If no guidance exists, the Derivative Classifier should refer to Chapter V, Paragraph 1d.
  - b. **National Security Information.** A Derivative Classifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the classifier's designation of authority. If no guidance exists, the Derivative Classifier should refer to Chapter V, Paragraph 1d. However, when information is extracted from a classified document, that document can be cited as a basis for classification if the information is entirely under the purview of another Government agency, a foreign government, or an international organization, and no joint classification guidance exists.
2. **REVIEW REQUIREMENTS.** Anyone who originates a document or material in a subject area that may be classified shall submit the document or material to the appropriate official for a classification review and determination prior to dissemination.
  - a. **Current Employee.**
    - (1) **Possesses an Active Access Authorization or Had One in the Past.**
      - (a) **Routine Document or Material.** An employee with an active access authorization who originates a document or material in a subject area that may be classified shall submit the document or material to a Derivative Classifier for classification review prior to dissemination. An employee who had an active access authorization in the past shall submit such a document or material to the local Classification Officer for classification review prior to dissemination. The local Classification

Officer may delegate this review responsibility to specified Derivative Classifiers.

- (b) Public Release or Widespread Distribution. A document or material that is prepared in a potentially classified subject area may be intended for public release or have such widespread internal distribution that public release is likely. In such cases, the originator shall submit the document or material to the local Classification Officer for classification review prior to dissemination. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
  - (c) Oral Presentations. An employee who is making an oral presentation in a subject area that may be classified shall submit the prepared text to the local Classification Officer for classification review prior to making the presentation. This includes any presentation made to the public as well as any presentation made to a sufficiently large, internal audience in an unclassified setting, making public release of the information likely. If the employee does not have a prepared text or if extemporaneous remarks are likely, the local Classification Officer shall brief the employee on classification guidance pertinent to the subject matter, including related topics the employee should avoid because they may be classified. The local Classification Officer may delegate this review and briefing responsibility to specified Derivative Classifiers.
- (2) Never Had an Access Authorization. An employee who has never had an access authorization may originate a document or material in a subject area that may be classified. In such cases, the local Classification Officer shall review the document or material for classification prior to dissemination. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
- b. Not an Employee.
- (1) Possesses an Active Access Authorization. The local Classification Officer shall review for classification a document or material that is submitted by an individual who is not employed by DOE, including NNSA, or their contractors but possesses an active access authorization. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
  - (2) Had an Access Authorization in the Past or Never Had an Access Authorization. The Director of Nuclear and National Security Information shall review for classification a document or material that is submitted by an individual who is not employed by DOE, including NNSA, or their contractors but had an access authorization in the past or has never had an access authorization.

3. **REQUIRED MARKINGS.** The Derivative Classifier shall ensure the following markings are included on the document or material being derivatively classified (see DOE M 471.2-1A, **MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL**, for complete information on marking requirements):
  - a. **Restricted Data/Formerly Restricted Data.**
    - (1) Overall classification level and category of the document.
    - (2) Classification level and category of each interior page of the document if not using the overall classification level and category on each page.
    - (3) Classification authority (i.e., "Classified By").
      - (a) Name or personal identifier of the Derivative Classifier.
      - (b) Position title of the Derivative Classifier.
    - (4) Designation of the guidance or source document(s) used to make the classification determination and the date of such document(s) (i.e., "Derived From").
  - b. **National Security Information.**
    - (1) Overall classification level of the document.
    - (2) Classification level of each interior page of the document if not using the overall classification level on each page.
    - (3) Portion marking for each section, part, paragraph, graphic, figure, or similar portion (for documents containing NSI only).
    - (4) Classification authority (i.e., "Classified By").
      - (a) Name or personal identifier of the Derivative Classifier.
      - (b) Position title of the Derivative Classifier.
    - (5) Designation of the guidance or source document(s) used to make the classification determination and date of such document(s) (i.e., "Derived From").
    - (6) Duration of classification derived from the guidance or source document(s) (i.e., "Declassify On").

- (a) Date - A specific date 10 years or less from the date of the document as specified by the guidance or source document(s).
  - (b) Event - A specific event occurring less than 10 years from the date of the document as specified by the guidance or source document(s).
  - (c) Exempt from declassification - Document is exempt from declassification at 10 years and identified by an exemption category (e.g., X1 through X8) as specified by the guidance or source document(s).
  - (d) Extension of classification - Classification of the document may be extended for successive periods not to exceed 10 years at a time. The "Declassify On" line shall be revised to include the date of the extension action, the new declassification date, and the person authorizing the extension.
  - (e) Reclassification - As appropriate, a document may be reclassified. The "Declassify On" line shall be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.
- c. Mixed Document. A mixed document contains both Restricted Data/Formerly Restricted Data information and National Security Information.
- (1) Overall classification level and category of the document (RD/FRD information takes precedence over NSI).
  - (2) Classification level and category (if RD or FRD) of each interior page of the document if not using the overall classification level and category on each page.
  - (3) Classification authority (i.e., "Classified By").
    - (a) Name or personal identifier of the Derivative Classifier.
    - (b) Position title of the Derivative Classifier.
  - (4) Designation of the guidance or source document(s) used to make the classification determination and the date of such document(s) (i.e., "Derived From").

4. PORTION MARKING REQUIREMENTS. NOTE: Derivative Classifiers and Declassifiers shall base their determinations on classification guidance pertaining to the specific subject areas

described in their designations of authority. If no guidance exists, they should refer to Chapter V, Paragraph 1d.

- a. Restricted Data/Formerly Restricted Data Documents. Documents containing only RD/FRD should not be portion-marked.
  - b. National Security Information Documents. Documents containing only NSI shall be portion-marked.
  - c. Mixed Documents. Documents containing both RD/FRD and NSI should not be portion-marked.
  - d. Documents Prepared Under Work-for-Others Contracts. Documents prepared under Work-for-Others contracts shall be portion-marked according to the rules stated in Paragraphs 4a through 4c above.
5. NOTIFICATION OF CLASSIFICATION. The Derivative Classifier who classifies a document shall notify the originator and provide sufficient information for the originator to identify the specific document being classified.
6. PROCEDURES RELATED TO THE REVIEW OF DOCUMENTS OR MATERIAL FOR CLASSIFICATION.
- a. Foreign Government Information. For additional information on marking documents containing foreign government information, refer to DOE M 471.2-1B, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
    - (1) Document or Material Generated by a Foreign Government. Review by a Derivative Classifier is not required to apply—
      - (a) a U.S. classification level that provides at least an equivalent level of protection to a document or material classified by the foreign government or
      - (b) the “Confidential—Modified Handling Authorized” marking to a document or material that the foreign government protects at a level lower than U.S. Confidential.
    - (2) Document or Material Generated by the United States. Review by a Derivative Classifier is required for a newly generated document or material concerning foreign government information that may also contain U.S. classified information.
  - b. Use of a Classified Addendum. To the maximum extent practical, the originator of a document containing classified information shall include the unclassified portions in the

5-8-98

primary document and shall separate the classified portions into attachments, appendixes, or supporting documents. If such separation is not practical and there is significant public interest in the document, the originator is encouraged to prepare an unclassified version.

- c. Review of Patent Applications and Reports.
- (1) Initial Review for Imposing a Secrecy Order. Section 151 of the Atomic Energy Act requires that no patent be granted for any invention or discovery that is useful solely in the utilization of special nuclear material or nuclear energy in a nuclear weapon. Also, any person making such an invention or discovery who does not file a patent application shall file a report with DOE that describes the invention or discovery. The Office of Nuclear and National Security Information shall review each patent application or report to determine whether it contains classified information and to impose a secrecy order on any application or report that does.
  - (2) Appeal of Secrecy Order Determination. If the person filing the patent application or report disputes the imposition of a secrecy order, the Director of Security Affairs shall review the application or report and determine whether the secrecy order was properly applied.
  - (3) Annual Review of Secrecy Order. On the anniversary date of imposing a secrecy order on a patent application or report, the Office of Nuclear and National Security Information shall confirm whether the secrecy order is still properly applied.
- d. External Coordination Reviews. A document or material being reviewed for classification may contain information under the cognizance of another Government agency or a foreign country. If the Derivative Classifier thinks the information may be classified and no guidance is available, he/she shall send the document or material to his/her Classification Officer for further review or referral to the Director of Nuclear and National Security Information.
- e. Classification Following Request for a Previously Unclassified Document. The public may request documents under a statute, Executive order, or regulation. Some of these documents may contain classified information, even though they are not so marked. Such documents shall be referred to the Director of Nuclear and National Security Information who shall review each one prior to its dissemination to determine if it may be classified. Documents containing only NSI that are more than 25 years old and that have been determined to be permanent records under Title 44 of the United States Code may not be classified under this provision.

## PART B - DECLASSIFICATION

Secretarial Officers and heads of DOE, including NNSA, Headquarters and field elements shall ensure that documents and material prepared under their purview are reviewed and processed in accordance with the provisions of this part.

1. **AUTHORITY.** A Derivative Declassifier may derivatively declassify a document or material originated in only those organizations and subject areas for which he/she has been delegated such authority and is governed by other limitations specified in the written designation. A Derivative Declassifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the declassifier's designation of authority. If no guidance exists, Derivative Declassifiers should refer to Chapter V, Paragraph 1d.
2. **REVIEW REQUIREMENTS FOR REDACTING A DOCUMENT OR DECLASSIFYING A DOCUMENT OR MATERIAL.** Preparing a redacted version of a document (i.e., a version of the document with all classified information removed) or declassifying a document or material in full requires two reviews by individuals who are knowledgeable in the subject area. The first review may be conducted by either a Derivative Classifier or Declassifier. The second review shall be conducted by a Derivative Declassifier (other than the first reviewer), who shall confirm that all classified information has been identified and bracketed in the document to be redacted or that the declassified document or material is unclassified.
3. **REQUIRED MARKINGS.** For each document or material that is declassified, the Derivative Declassifier shall ensure that the following markings are included on the document or material and that the classification markings are crossed out:
  - a. date of declassification (i.e., "Declassified On");
  - b. name(s) and position(s) or title(s) of individual(s) declassifying the document (i.e., "Declassified By");
  - c. designation of the guidance or source document(s) used as the basis for the declassification determination and the date of such document(s) (i.e., "Derived From").
4. **DURATION OF CLASSIFICATION.**
  - a. **Restricted Data/Formerly Restricted Data.** Documents or material containing RD/FRD are never automatically declassified. Such documents or material remain classified until an authorized person takes positive action to declassify them. Under the Atomic Energy Act, no date or event for automatic declassification ever applies to RD/FRD documents or material, even if such documents or material also contain NSI.
  - b. **National Security Information.** DOE, including NNSA, documents marked as containing NSI that do not specify a date or event for declassification are never

automatically declassified. Section 3155(a) of Public Law 104-106 states that before such a document can be released or declassified, it shall be reviewed to determine if it contains RD/FRD. If the document contains RD/FRD, it shall be so marked and may only be declassified under the provisions in Paragraph 4a above. However, if the document is determined to contain only NSI, the following paragraphs apply:

- (1) Marked with Specific Date or Event for Declassification. A document marked with a specific date or event for declassification is declassified after the date or event has passed. Anyone may remove or obliterate the classification markings on such a document.
- (2) Exemption from Declassification within 10 Years. A document marked as exempt from declassification within 10 years is not automatically declassified. Procedures for such a document are contained in Part B, Paragraph 2, above.
- (3) Historical Records.
  - (a) Permanent Records. If a document contains only NSI, is more than 25 years old, and has been determined to be a permanent record under Title 44 of the United States Code, a Derivative Declassifier shall determine if the document can be declassified or if it is exempt from the automatic declassification requirements based on guidance in the Historical Records Declassification Guide.
  - (b) Temporary and Unscheduled Records. A document that contains only NSI, is more than 25 years old, and has been determined to be a temporary record or is an unscheduled record is not subject to the automatic declassification requirements in this paragraph (i.e., Paragraph 4). Such a document retains its current classification status until it is reviewed using current classification guidance and determined to be unclassified under the procedures in Paragraph 2 above. (NOTE: Unscheduled records have not been determined to be either permanent or temporary.)

## 5. TYPES OF DOCUMENT REVIEWS.

### a. Freedom of Information Act Requests.

- (1) Initial Requests. A classified document requested under the Freedom of Information Act is reviewed in accordance with the provisions of 10 CFR Part 1004 and this Manual. The Director of Nuclear and National Security Information shall concur on all responses involving the denial of a classified document and shall serve as the Denying Official for any classified portion of such a document. (The Director of Nuclear and National Security Information may delegate this responsibility to another DOE, including NNSA, official.)

(2) Appeals of Denials.

- (a) Authority. The Director of Security Affairs shall make the final appeal determination to release any portion of a document previously denied because it was classified. The Director of Hearings and Appeals shall issue the final appeal determination on behalf of DOE, including NNSA.
- (b) Analytical Support. The Director of Nuclear and National Security Information shall provide analytical support and recommendations to assist the Director of Security Affairs in exercising his/her appeal authority.

b. Privacy Act Requests.

- (1) Initial Requests. A classified document requested under the Privacy Act is reviewed in accordance with the provisions of 10 CFR Part 1008 and this Manual. The Director of Nuclear and National Security Information shall concur on all responses involving the denial of a classified document and shall make the final determination concerning the denial of any classified portion of such a document. (The Director of Nuclear and National Security Information may delegate this responsibility to another DOE, including NNSA, official.)

(2) Appeals of Denials.

- (a) Authority. The Director of Security Affairs shall make the final appeal determination to release any portion of the document previously denied because it was classified. The Director of Hearings and Appeals shall issue the final appeal determination on behalf of DOE, including NNSA.
- (b) Analytical Support. The Director of Nuclear and National Security Information shall provide analytical support and recommendations to assist the Director of Security Affairs in exercising his/her appeal authority.

c. Mandatory Review Requests.

- (1) Initial Request. Any employee who receives a mandatory review request for a document containing RD/FRD information or NSI shall send the request to the local Classification Officer for review and transmittal to the Director of Nuclear and National Security Information for processing.
- (2) Appeal of Denials.

- (a) Restricted Data/Formerly Restricted Data. The Director of Security Affairs shall make the final appeal determination on any RD/FRD portion of a document that was previously denied by DOE, including NNSA.
  - (b) National Security Information. The Director of Security Affairs shall make the appeal determination on any NSI portion of a document that was previously denied. If such determination has not been received within 180 working days of filing the appeal or if the requester is dissatisfied with the final determination, the requester may seek further review by the Interagency Security Classification Appeals Panel, as described in Appendix A to 32 CFR Part 2001.
- d. Systematic Reviews. The Director of Nuclear and National Security Information oversees the systematic review program for classified documents originated by DOE, including NNSA.
  - (1) Restricted Data/Formerly Restricted Data. The local classification office shall ensure that documents containing RD/FRD information are periodically and systematically reviewed for declassification. Such reviews shall be based on the degree of public and researcher interest and the likelihood of declassification upon review.
  - (2) National Security Information. The local classification office shall ensure that documents containing NSI that have been exempted from automatic declassification are periodically and systematically reviewed for declassification. Such reviews shall be based on the degree of public and researcher interest and the likelihood of declassification upon review.
- e. Other Reviews. The local classification office shall ensure that documents or material containing RD/FRD information or NSI are reviewed for declassification for any reason other than those defined in Paragraphs 5a-5d above (e.g., congressional testimony, litigation, and reviews to preclude erroneous automatic declassification).

## 6. DOCUMENT REVIEW PLAN.

- a. Determining Need for a Plan. The Classification Officer shall notify the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements) whenever a group of documents to be reviewed for declassification exceeds 10,000 pages. Such notification shall describe why the review is necessary, estimate the number of pages or volume of material requiring review, and describe the anticipated impact on resources. After consulting with the Classification Officer, the Director of Nuclear and National Security Information shall determine if the Classification Officer needs to develop a document review plan.

- b. Contents of the Plan. The plan shall--
- (1) describe why the review is required;
  - (2) contain detailed, written procedures that describe how the technical and administrative aspects of the review will be conducted;
  - (3) contain a statistically valid quality assurance assessment plan with standards for remedial action specified;
  - (4) summarize exceptions and deviations from standards;
  - (5) provide the names and classification/declassification authorities of the reviewers;
  - (6) list the classification guidance to be used; and
  - (7) contain a sample of the stamps to be used.
- c. Submission and Approval of the Plan. The Classification Officer shall submit the plan to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements) for approval prior to starting work.

7. NOTIFICATION OF DECLASSIFICATION. For documents less than 25 years old, the Derivative Declassifier who declassifies a document shall notify the originator or document custodian to the maximum extent possible and provide sufficient information for the originator or document custodian to identify the specific document being declassified.

8. PROCEDURES RELATED TO THE DECLASSIFICATION REVIEW OF DOCUMENTS OR MATERIAL.

- a. Public Release. Declassifying a document or material does not mean that it may be released to the public automatically. Information contained in the document or material may still be exempt from release for other reasons; therefore, once a document or material is declassified, it must still be reviewed to determine if the information falls within any of the Freedom of Information Act exemptions before it can be released to the public.
- b. External Coordination Reviews.
- (1) DOE, including NNSA, Documents or Material. Prior to declassifying a document or material containing information under the cognizance of another DOE, including NNSA, element, a Derivative Declassifier shall either send the document or material to that organization for review or obtain the concurrence of that organization that the document or material can be declassified unless specific authority to declassify the document or material has been delegated.

- (2) Other Agency Documents. The Director of Nuclear and National Security Information shall conduct any interagency coordination required to declassify a document or material containing RD/FRD information or NSI when the document or material relates to litigation or has been requested under the Freedom of Information Act. In all other cases, Classification Officers shall conduct any interagency coordination required to declassify a document or material containing either RD/FRD information or NSI. To assist with this coordination, the Office of Nuclear and National Security Information shall provide Classification Officers with the names and addresses of appropriate interagency points of contact.
  - (3) Foreign Government and International Organization Documents or Material. Unless public release is specifically authorized through current classification guidance, the Director of Nuclear and National Security Information shall conduct all coordination required to declassify a document or material that contains information—
    - (a) provided to the United States by a foreign government or international organization or
    - (b) produced by the United States under a joint arrangement with a foreign government or international organization.
- c. OpenNet Data Base. Each organization that declassifies a document and determines that it may be released to the public shall ensure that the following information is submitted to the Office of Scientific and Technical Information for inclusion on the OpenNet data base:
- (1) a bibliographic reference to the document and
  - (2) the location where the document is available to the public.
- d. Obsolete Classification Markings. Documents dated prior to December 15, 1953, and marked as “Restricted” and documents dated between July 18, 1949, through October 22, 1951, and marked as “Official Use Only” were considered classified. However, these markings are either no longer used or have a different meaning.
- (1) Review Requirements. A Derivative Classifier or Declassifier (only one review is required) shall review such documents to determine their current classification status. Until that review is completed, the documents shall be marked and protected according to DOE M 471.2-1B, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
  - (2) Determined to be Classified. If a Derivative Classifier determines the documents are classified, the “Restricted” or “Official Use Only” markings shall

be crossed out and replaced with current classification markings. The Derivative Classifier shall prepare an upgrading notice, as appropriate.

- (3) Determined Not to be Classified. If a Derivative Classifier or Declassifier determines the documents are not classified, the "Restricted" or "Official Use Only" markings shall be crossed out and replaced with the marking "Unclassified," along with the name of the reviewer. A declassification notice is not required.
  
- e. Extracted Version of Document. A major portion of an existing classified document (i.e., a chapter or appendix) may be extracted for use as a new document. Such a document shall be clearly identified as an extract and shall be marked and protected according to DOE M 471.2-1B, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL. A Derivative Classifier shall review the new document to determine if it contains classified information.
  
- f. Redacted Version of Document. A redacted document shall clearly indicate it is a redacted version.
  
- g. Review Upon Termination of Employment. A DOE, including NNSA, employee who retires or otherwise terminates employment may wish to take correspondence, personal records, diaries, or other documents with him/her. If these records fall wholly or partially in areas that are classified, a review by a Derivative Classifier is required.

**PART C - DOWNGRADING OR UPGRADING****1. GENERAL.**

- a. Downgrading occurs when an appropriate authority determines the document or material can be adequately protected at a classification level or category lower than currently marked, not including "Unclassified." (Downgrading to "Unclassified" is called declassifying, which is covered under Part B of this chapter.)
- b. Upgrading occurs when an appropriate authority—
  - (1) assigns the appropriate classification level and/or category to a document or material erroneously issued as unclassified or
  - (2) raises the classification level or category of a document or material to protect the contents adequately.

**2. AUTHORITY.**

- a. Downgrading. A Derivative Declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of notice from the proper authority.
- b. Upgrading. A Derivative Classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of notice from the proper authority.

**3. NOTIFICATION OF DOWNGRADING OR UPGRADING.**

- a. Downgrading. The Derivative Declassifier authorizing the downgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being downgraded.
- b. Upgrading. The Derivative Classifier authorizing the upgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being upgraded. The Derivative Classifier shall refer to appropriate classification guidance when preparing upgrading notices because such notices may be classified.

## PART D - RECLASSIFICATION

### 1. AUTHORITY.

- a. General. A Derivative Classifier may reclassify a document or material within his/her designated authority.
- b. Following Request for a Previously Declassified Document. The public may request declassified documents under a statute or Executive order. Some of these documents may inadvertently still contain classified information. Such documents shall be referred to the Director of Nuclear and National Security Information, who shall review each one prior to its dissemination to determine if it may be reclassified. Documents containing only NSI that are more than 25 years old and that have been determined to be permanent records under Title 44 of the United States Code may not be reclassified under this provision.

2. NOTIFICATION OF RECLASSIFICATION. The Derivative Classifier authorizing the reclassification of a document or material shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document or material being reclassified. The Derivative Classifier shall refer to appropriate classification guidance when preparing a reclassification notice because such notices are usually classified.

## CHAPTER VII

### EDUCATION PROGRAM

1. INITIAL CLASSIFICATION EDUCATION. All cleared DOE, including NNSA, employees must understand their classification/declassification responsibilities. Each Classification Officer shall ensure that such employees receive a classification orientation that includes identification of a point of contact to answer questions or address concerns about classification or declassification matters.
2. CONTINUING EDUCATION. Each Classification Officer shall ensure that a continuing classification education program is conducted annually for all cleared employees to maintain classification awareness and inform them of applicable changes in classification policies, principles, guidance, and procedures.
3. INITIAL TRAINING FOR A CLASSIFIER OR DECLASSIFIER. Before becoming Original Classifiers, Derivative Classifiers, or Derivative Declassifiers, individuals shall receive training covering the following elements and shall successfully complete an examination to ensure they understand these elements sufficiently:
  - a. Original Classifier:
    - (1) the difference between original and derivative classification,
    - (2) who can classify information originally,
    - (3) the standards that an Original Classifier must apply to classify information,
    - (4) the process for determining the duration of classification,
    - (5) the prohibitions and limitations on classifying information,
    - (6) the basic markings that must appear on an originally classified document, and
    - (7) the general standards and procedures for declassification.
  - b. Derivative Classifier:
    - (1) the process of original and derivative classification and the standards applicable to each,
    - (2) the markings that must appear on a derivatively classified document, and
    - (3) the authorities, methods, and processes for downgrading and declassifying information, documents, and material.

- c. Derivative Declassifier:
- (1) the standards, methods, and procedures for declassifying documents or material under the Atomic Energy Act and Executive Order 12958,
  - (2) the standards for using declassification guidance,
  - (3) the markings that must appear on a derivatively declassified document,
  - (4) the contents of an applicable declassification plan, and
  - (5) responsibilities for establishing and maintaining a declassification data base.
4. RECERTIFICATION TRAINING. To recertify as an Original Classifier, Derivative Classifier, or Derivative Declassifier, an individual shall successfully complete an examination that, at a minimum, retests his/her understanding of applicable classification and declassification policies, principles, procedures, and guidance.

## CHAPTER VIII

### CLASSIFICATION AND DECLASSIFICATION OVERSIGHT PROGRAM

1. PERFORMANCE OBJECTIVE. The Office of Nuclear and National Security Information manages the classification and declassification oversight program that ensures that all DOE, including NNSA, and their contractor and subcontractor organizations that generate classified information and documents or material have implemented and maintain an adequate and effective classification and declassification program.
2. SCOPE.
  - a. Differing Scope and Complexity. Classification and declassification programs at various facilities differ in scope and complexity. No single list of areas to be covered in an oversight review is appropriate in all cases. Therefore, the scope of the oversight review must be tailored to ensure that it provides the management and oversight necessary to evaluate the adequacy and effectiveness of each individual classification and declassification program.
  - b. Uniformity of Oversight Reviews. To introduce a measure of uniformity into classification and declassification oversight reviews, each review shall cover, at a minimum, the following areas:
    - (1) management awareness and support,
    - (2) document reviews,
    - (3) guidance,
    - (4) education,
    - (5) classifiers and declassifiers,
    - (6) declassification,
    - (7) effectiveness of the program to publicly release declassified documents, and
    - (8) oversight reviews of contractors.
3. FREQUENCY OF OVERSIGHT REVIEWS. The frequency of oversight reviews is determined after considering the following factors:
  - a. Past Performance Experience and Review Results. More frequent reviews are conducted of facilities that have experienced problems previously.
  - b. Interval Since Last Review. Facilities having a major classification and declassification interest are reviewed every 2 years unless particular circumstances indicate otherwise. Facilities with effective classification and declassification programs or minor interests may be reviewed less frequently (every 3-5 years). The local Classification Officer shall determine the frequency of oversight reviews of subordinate facilities.

4. OVERSIGHT REVIEW REPORTS. The oversight review report shall ensure the organization reviewed receives a clear explanation of its performance. The review report shall ensure that deficiencies or problem areas are identified.
5. FOLLOW-UP MEASURES. Follow-up measures shall ensure that the actions taken to correct deficiencies noted during an oversight review are adequate and have been implemented in a timely manner.
6. SELF-ASSESSMENTS. Each DOE, including NNSA, element that generates classified information and documents or material shall establish and maintain an ongoing self-assessment program, documented in writing to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements). Self-assessments shall be conducted annually unless prior agreement is reached with the Director of Nuclear and National Security Information.

## DEFINITIONS

1. Automatic Declassification. The declassification of a document or material based solely upon the occurrence of a specific date or event as determined by classification guidance or the expiration of a maximum time frame for duration of classification established under Executive Order 12958.
2. Classification Guidance. A written record of detailed instructions as to whether specific information is classified, usually concerning a system, plan, project, or program. The guidance identifies information to be classified and specifies the level (and duration for National Security Information only) of classification assigned to such information. Classification guidance is the primary basis for reviewing documents or material to determine whether they contain classified information.
3. Classification Officer.
  - a. Headquarters Classification Officer. The Director of Nuclear and National Security Information.
  - b. Field Element Classification Officer. An individual designated to administer the classification program for that particular field element and to monitor the classification programs of contractors under its cognizance.
  - c. Contractor Classification Officer. An individual designated to administer the classification program for that particular contractor and to monitor the classification programs of subcontractors under its cognizance.
  - d. Local Classification Officer. For DOE and NNSA Headquarters elements, the Director of Nuclear and National Security Information is the local Classification Officer. For field elements with no designated Classification Officer, the Director of Nuclear and National Security Information is the local Classification Officer. For contractors with no designated Classification Officer, the appropriate field element Classification Officer is the local Classification Officer.
4. Classified Information. Information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, as amended, or information determined to require protection against unauthorized disclosure under Executive Order 12958 or prior Executive orders, which is identified as National Security Information.
5. Declassification. A determination by an appropriate authority that information or documents and material no longer require protection as classified information against unauthorized disclosure because of national security concerns.
6. Denying Official. An individual, designated under 10 CFR Part 1004, who is authorized to make the final decision on what information contained in a document requested under the Freedom of Information Act may be withheld.
7. Derivative Classification. A determination based on classification guidance or source documents that a document or material contains Restricted Data, Formerly Restricted Data, and/or National Security Information.

8. Derivative Classifier. An individual authorized to determine that a document or material is unclassified or classified as Restricted Data, Formerly Restricted Data, and/or National Security Information and at what level based on classification guidance or source documents. (A Derivative Classifier is equivalent to the Restricted Data Classifier referred to in 10 CFR Part 1045.)
9. Derivative Declassifier. An individual authorized to declassify or downgrade documents or material in specified areas based on classification or declassification guidance or source documents.
10. Document. Written or printed information; removable ADP media (diskettes, tapes, cards, etc); charts; maps; paintings; drawings; engravings; sketches; photographic prints; exposed or developed film; working notes and papers; reproductions of such things by any means or process; and sound and video recordings generated by magnetic, optical, or any other electronic means.
11. Downgrading. A determination by an appropriate authority that (a) information may be protected at a level lower than the initial classification level or (b) a document or material may be protected at a level and/or category lower than the initial classification level and/or category. In either case, however, the revised classification level shall not be lower than Confidential.
12. Foreign Government Information. Such information consists of one of the following:
  - a. information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
  - b. information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
  - c. information received and treated as "Foreign Government Information" under the terms of a predecessor order.
13. Formerly Restricted Data (FRD). Classified information jointly determined by the Director of Security Affairs and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the Director of Security Affairs from the Restricted Data category pursuant to Section 142(d) of the Atomic Energy Act, as amended, and safeguarded as National Security Information, subject to restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.
14. Headquarters Classification Representative. An individual designated by his/her Headquarters element to serve as the point of contact with the Office of Nuclear and National Security Information on classification and declassification policies and procedures and to assist others in his/her Headquarters element with their classification and declassification responsibilities and authorities.

15. Information. Facts, data, or knowledge itself as opposed to the medium in which it is contained.
16. Local classification office. The organization within a field element that is responsible for handling classification/declassification-related issues.
17. Mandatory Review. A declassification review of a document containing RD/FRD information that is requested under 10 CFR Part 1045.42, or a document containing NSI that is requested under Section 3.6 of Executive Order 12958.
18. Material. Any substance regardless of its physical or chemical form, including any raw, in-process, or manufactured commodity, equipment, component, accessory, part, assembly, or product of any kind.
19. National Security Information (NSI). Information that has been determined pursuant to Executive Order 12958 and any predecessor orders to require protection against unauthorized disclosure and that is so designated. The levels Top Secret, Secret, and Confidential are used to designate such information.
20. Official Use Only.
  - a. A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act.
  - b. A security classification marking used from July 18, 1949, through October 22, 1951.
21. Original Classification. A determination by an Original Classifier that certain new information requires protection against unauthorized disclosure because of national security interests under Executive Order 12958; such information is identified as National Security Information.
22. Original Classifier. A Federal Government employee who is authorized to determine under Executive Order 12958 that certain new information requires protection against unauthorized disclosure in the interest of national security; such information is identified as National Security Information.
23. Permanent Records. Records appraised by the National Archives and Records Administration under Title 44 of the United States Code and determined to have sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes.
24. Portion Marking. The application of certain classification markings to individual words, phrases, sentences, paragraphs, or sections of a document to indicate their specific classification level and category (if RD or FRD).
25. Reclassification. A determination by an appropriate authority that restores the classification to (a) information that was classified as NSI and then declassified or (b) a document or material that was classified as RD, FRD, or NSI and then erroneously declassified.
26. Restricted Data (RD). All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the

production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

27. Source Document. A classified document, other than classification guidance, from which information is extracted for inclusion in another document. Classification of the information extracted is determined by the classification markings shown in the source document.
28. Systematic Review. A periodic review of classified documents for declassification based on the degree of public and researcher interest and the likelihood of declassification upon review.
29. Upgrading. A determination by an appropriate authority that (a) assigns the correct classification level and/or category to a document or material that was erroneously issued as unclassified or (b) raises the classification level or category of a document or material to adequately protect the contents.
30. Variance. A method that differs from a directive requirement for a specific or indefinite period of time or for a specific project, but still meets that requirement by providing an equivalent level of implementation.
31. Waiver. Exemption from meeting a specific directive requirement.

## CONTRACTOR REQUIREMENTS DOCUMENT

### DOE M 475.1-1A, IDENTIFYING CLASSIFIED INFORMATION

1. **PURPOSE.** This Contractor Requirements Document (CRD) provides requirements for managing the contractor's classification and declassification program, including details for classifying and declassifying information, documents, and material. This CRD supplements DOE M 475.1-1A, IDENTIFYING CLASSIFIED INFORMATION.
2. **USAGE.** This CRD is divided into the following chapters:
  - a. **Chapter I - Program Administration.** Part A contains qualification and designation requirements for Classification Officers, Original Classifiers, Derivative Classifiers, and Derivative Declassifiers. Part B contains administrative policies that apply to the overall Department of Energy (DOE) classification and declassification program.
  - b. **Chapter II - Classification Categories and Levels.** Provides an overview of the categories of classified information and what levels may be applied to these categories.
  - c. **Chapter III - Classifying and Declassifying Information.** Classifying, declassifying, downgrading or upgrading, or reclassifying information is a function performed by Federal Government officials only; however, this chapter describes activities that require input from contractors.
  - d. **Chapter IV - Classification Guidance.** Describes the DOE classification guidance system, which specifies the information that is classified and unclassified.
  - e. **Chapter V - Classifying and Declassifying Documents and Material.** Describes how documents and material are classified, declassified, downgraded or upgraded, or reclassified. Requirements in this chapter are applied by originators of documents and material, Derivative Classifiers, Derivative Declassifiers, Classification Officers, Headquarters Classification Representatives, the Director of Nuclear and National Security Information, and the Director of Security Affairs.
  - f. **Chapter VI - Education Program.** Describes training needed by Derivative Classifiers, Derivative Declassifiers, and other contractor employees who generate classified information.
  - g. **Chapter VII - Classification and Declassification Oversight Program.** Describes elements of the oversight program to ensure that organizations generating classified information, documents, and material maintain an adequate and effective classification and declassification program.

3. DEFINITIONS. Definitions of terms used throughout this CRD can be found in Chapter VIII.
4. CONTACT. Questions concerning this document should be addressed to the Policy and Quality Management Division, Office of Nuclear and National Security Information (301-903-5454).

## CONTENTS

### CHAPTER I - PROGRAM ADMINISTRATION

#### PART A - QUALIFICATIONS AND DESIGNATIONS ..... I-1

1.	Classification Officer. ....	I-1
	a. Requirement for Position .....	I-1
	b. Qualifications .....	I-1
	c. Nomination .....	I-1
	d. Training Requirement .....	I-2
	e. Removal from Position .....	I-2
2.	Original Classifier .....	I-2
3.	Derivative Classifier .....	I-2
	a. Qualifications .....	I-2
	b. Designation Process .....	I-3
	c. Duration of Authority .....	I-4
	d. Redlegation .....	I-4
	e. Cancellation of Authority .....	I-4
	f. Notification of Vacant Position .....	I-5
4.	Derivative Declassifier .....	I-5
	a. Qualifications .....	I-6
	b. Designation Process .....	I-6
	c. Duration of Authority .....	I-7
	d. Redlegation .....	I-7
	e. Cancellation of Authority .....	I-7
	f. Notification of Vacant Position .....	I-7

#### PART B - ADMINISTRATIVE POLICIES ..... I-9

1.	Performance Standards .....	I-9
2.	Challenges to Classification .....	I-9
	a. Restricted Data/Formerly Restricted Data .....	I-9
	b. National Security Information .....	I-9
3.	Reporting Requirements .....	I-10
4.	Misclassification of Information, Documents, or Material .....	I-10
	a. Deliberate Action .....	I-10
	b. Negligence in Exercising Classification/Declassification Authority .....	I-10
5.	Deviations from Requirements .....	I-10

### CHAPTER II - CLASSIFICATION CATEGORIES AND LEVELS

1.	Categories of Classified Information .....	II-1
	a. Restricted Data and Formerly Restricted Data .....	II-1
	b. National Security Information .....	II-1

**CONTENTS (continued)**

2.	Levels of Classification .....	II-1
a.	Top Secret .....	II-1
b.	Secret .....	II-1
c.	Confidential .....	II-1
3.	Use of the Term "Unclassified" .....	II-2

**CHAPTER III - CLASSIFYING AND DECLASSIFYING INFORMATION**

1.	Request for Determination .....	III-1
2.	Unauthorized Disclosure .....	III-1
3.	Declassification Proposals .....	III-1
a.	Ad Hoc Proposals .....	III-1
b.	Disposition of Proposal .....	III-1

**CHAPTER IV - CLASSIFICATION GUIDANCE**

1.	General .....	IV-1
a.	Purpose .....	IV-1
b.	Content .....	IV-1
c.	Inconsistent Guidance .....	IV-1
d.	No Guidance .....	IV-1
2.	Types of Guidance .....	IV-2
a.	Headquarters Guidance .....	IV-2
b.	Local Guidance .....	IV-2
3.	Related Policies and Procedures .....	IV-3
a.	Updating Guidance .....	IV-3
b.	Classification Guidance for DOE Contractors .....	IV-4
c.	Classification Guidance for Non-DOE, Including non-NNSA, Funded Work .....	IV-4

**CHAPTER V - CLASSIFYING AND DECLASSIFYING DOCUMENTS AND MATERIAL**

<b>PART A - CLASSIFICATION .....</b>		<b>V-1</b>
1.	Authority .....	V-1
a.	Restricted Data/Formerly Restricted Data .....	V-1
b.	National Security Information .....	V-1
2.	Review Requirements .....	V-1
a.	Current Employee .....	V-1
b.	Not an Employee .....	V-2
3.	Required Markings .....	V-2
a.	Restricted Data/Formerly Restricted Data .....	V-3
b.	National Security Information .....	V-3
c.	Mixed Document .....	V-4

**CONTENTS (continued)**

4. Portion Marking Requirements ..... V-4  
    a. Restricted Data/Formerly Restricted Data Documents ..... V-4  
    b. National Security Information Documents ..... V-5  
    c. Mixed Documents ..... V-5  
    d. Documents Prepared Under Work-for-Others Contracts ..... V-5  
5. Notification of Classification ..... V-5  
6. Procedures Related to the Review of Documents or Material for Classification ..... V-5  
    a. Foreign Government Information ..... V-5  
    b. Use of a Classified Addendum ..... V-5  
    c. External Coordination Reviews ..... V-6  
    d. Classification Following Request for a Previously Unclassified Document ..... V-6

**PART B - DECLASSIFICATION ..... V-7**

1. Authority ..... V-7  
2. Review Requirements for Redacting a Document or Declassifying  
    a Document or Material ..... V-7  
3. Required Markings ..... V-7  
4. Duration of Classification ..... V-7  
    a. Restricted Data/Formerly Restricted Data ..... V-7  
    b. National Security Information ..... V-7  
5. Types of Document Reviews ..... V-8  
    a. Mandatory Review Requests ..... V-8  
    b. Systematic Reviews ..... V-8  
    c. Other Reviews ..... V-9  
6. Document Review Plan ..... V-9  
    a. Determining Need for a Plan ..... V-9  
    b. Contents of the Plan ..... V-9  
    c. Submission and Approval of the Plan ..... V-10  
7. Notification of Declassification ..... V-10  
8. Procedures Related to the Declassification Review of Documents or Material ..... V-10  
    a. Public Release ..... V-10  
    b. External Coordination Reviews ..... V-10  
    c. OpenNet Data Base ..... V-11  
    d. Obsolete Classification Markings ..... V-11  
    e. Extracted Version of Document ..... V-11  
    f. Redacted Version of Document ..... V-12  
    g. Review Upon Termination of Employment ..... V-12

**PART C - DOWNGRADING OR UPGRADING ..... V-13**

1. General ..... V-13

**CONTENTS (continued)**

2. Authority ..... V-13  
    a. Downgrading ..... V-13  
    b. Upgrading ..... V-13  
3. Notification of Downgrading or Upgrading ..... V-13  
    a. Downgrading ..... V-13  
    b. Upgrading ..... V-13

**PART D - RECLASSIFICATION ..... V-15**

1. Authority ..... V-15  
    a. General ..... V-15  
    b. Following Request for a Previously Declassified Document ..... V-15  
2. Notification of Reclassification ..... V-15

**CHAPTER VI - EDUCATION PROGRAM**

1. Initial Classification Education ..... VI-1  
2. Continuing Education ..... VI-1  
3. Initial Training for a Classifier or Declassifier ..... VI-1  
    a. Derivative Classifier ..... VI-1  
    b. Derivative Declassifier ..... VI-1  
4. Recertification Training ..... VI-1

**CHAPTER VII - CLASSIFICATION AND DECLASSIFICATION OVERSIGHT PROGRAM**

1. Performance Objective ..... VII-1  
2. Scope ..... VII-1  
    a. Differing Scope and Complexity ..... VII-1  
    b. Uniformity of Oversight Reviews ..... VII-1  
3. Frequency of Oversight Reviews ..... VII-1  
    a. Past Performance Experience and Review Results ..... VII-1  
    b. Interval Since Last Review ..... VII-2  
4. Oversight Review Reports ..... VII-2  
5. Follow-up Measures ..... VII-2  
6. Self-Assessments ..... VII-2

**CHAPTER VIII - DEFINITIONS ..... VIII-1**

## CHAPTER I

### PROGRAM ADMINISTRATION

#### PART A - QUALIFICATIONS AND DESIGNATIONS

##### 1. CLASSIFICATION OFFICER.

###### a. Requirement for Position.

- (1) Contractor. The requirement for a contractor Classification Officer is determined by the cognizant field element Classification Officer.
- (2) Subcontractor. The contractor Classification Officer shall determine when a subcontractor under his/her cognizance is required to designate a Classification Officer.

b. Qualifications. A Classification Officer must have a scientific or technical degree related to the field in which he/she is working. The Director of Nuclear and National Security Information may waive this requirement for nominees with suitable experience. Each contractor Classification Officer shall also be a Derivative Classifier and a Derivative Declassifier.

###### c. Nomination.

- (1) Contractor. The head of a contractor organization shall nominate an individual for the position of Classification Officer by submitting that individual's name and qualifications to the appropriate field element Classification Officer. The field element Classification Officer submits the nomination to the Director of Nuclear and National Security Information with a recommendation for approval if the qualifications are adequate. For NNSA elements, the nomination must be submitted through the Chief of Defense Nuclear Security. If the qualifications are not adequate, the field element Classification Officer returns the request to the head of the contractor organization for reconsideration.
- (2) Subcontractor. The head of a subcontractor organization shall nominate an individual for the position of Classification Officer by submitting that individual's name and qualifications to the contractor Classification Officer. The contractor Classification Officer shall submit the nomination to the Director of Nuclear and National Security Information, through the appropriate field element Classification Officer, with a recommendation for approval if the qualifications are adequate. For NNSA elements, the nomination must be submitted through the Chief of Defense Nuclear Security. If the qualifications are not adequate,

the contractor Classification Officer shall return the request to the head of the subcontractor organization for reconsideration.

- d. Training Requirement. Approval by the Director of Nuclear and National Security Information is contingent upon the nominee successfully completing the training course prepared and presented by the Office of Nuclear and National Security Information.
  - e. Removal from Position. The head of the contractor/subcontractor organization, the Chief of Defense Nuclear Security, or the Director of Nuclear and National Security Information may remove an employee from the Classification Officer's position when the employee cannot or does not perform his/her responsibilities reliably.
    - (1) Removal by the Head of the Contractor/Subcontractor Organization. The head of the contractor/subcontractor shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the removal, the reason for removal, and the effective date.
    - (2) Removal by the Chief of Defense Nuclear Security. The Chief of Defense Nuclear Security shall notify the employee and inform the head of the contractor/ subcontractor organization and the Director of Nuclear and National Security Information of the removal, the reason for removal, and the effective date.
    - (3) Removal by the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information notifies the employee and informs the head of the contractor/subcontractor organization (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the removal, the reason for removal, and the effective date.
2. ORIGINAL CLASSIFIER. Original classification authority is delegated only to Federal employees occupying positions with an established need for such authority.
  3. DERIVATIVE CLASSIFIER. Classification Officers designate specific individuals as Secret and Confidential Derivative Classifiers. These individuals may exercise derivative classification authority only while occupying those positions for which the authority was granted. This authority may not be assumed by an individual serving in an acting capacity. This authority is not retained when the individual transfers to another position. If an individual vacates a position that requires derivative classification authority, the individual who will permanently fill the vacancy is not automatically granted the authority, but is designated only in accordance with the procedures in Paragraph 3b below.
    - a. Qualifications. To be nominated as a Derivative Classifier, an employee shall-

- (1) have demonstrated competence in the subject area in which the authority will be used and
- (2) be familiar with DOE classification policy and procedures, especially in the subject area for which the authority will be used.

b. Designation Process.

- (1) Designating Official.
  - (a) Top Secret Derivative Classifiers. The Director of Nuclear and National Security Information designates all Top Secret Derivative Classifiers.
  - (b) Secret and Confidential Derivative Classifiers. Each contractor Classification Officer shall designate Secret and Confidential Derivative Classifiers for contractor and subcontractor organizations under his/her purview and shall maintain a current list of such designations.
- (2) Request for Designation. The employee's supervisor or higher authority shall submit a request to the designating official following instructions issued by the local classification office.
- (3) Evaluation of Request. The designating official shall evaluate the need for the authority and the qualifications of the individual.
- (4) Required Training.
  - (a) New Derivative Classifier. Prior to being designated as a Derivative Classifier, each employee shall successfully complete a training program and examination specified by the designating official.
  - (b) Derivative Classifier Recertification. To recertify as a Derivative Classifier, an employee shall successfully complete an examination specified by the designating official.
  - (c) Waiver of Required Training. The designating official may waive the required training and examination for an employee who has met the requirements within the last 3 years and who is transferring from a similar programmatic position.
- (5) Designation. The designating official shall designate in writing each Derivative Classifier. Each designation shall describe the specific subject areas covered by the Derivative Classifier's authority and state the date the authority expires.

- c. Duration of Authority. Derivative classification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.
- d. Redelegation. Derivative classification authority cannot be redelegated.
- e. Cancellation of Authority.
  - (1) Top Secret. The employee's supervisor, the Chief of Defense Nuclear Security, or the Director of Nuclear and National Security Information may cancel Top Secret derivative classification authority when the employee's position no longer requires such authority, or the employee cannot or does not exercise that authority reliably.
    - (a) By the Employee's Supervisor. The supervisor who cancels Top Secret derivative classification authority for an employee under his/her cognizance shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the employee's name and position, the reason for cancellation, and the date the authority will end.
    - (b) By the Chief of Defense Nuclear Security. Upon canceling the Top Secret derivative classification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the employee's supervisor and the Director of Nuclear and National Security Information of the employee's name and position, the reason for cancellation, and the date the authority will end.
    - (c) By the Director of Nuclear and National Security Information. Upon canceling the Top Secret derivative classification authority for an employee, the Director of Nuclear and National Security Information notifies the employee and informs the employee's supervisor (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the employee's name and position, the reason for cancellation, and the date the authority will end.
  - (2) Secret and Confidential. The employee's supervisor, the designating official, the field element Classification Officer for contractors under his/her cognizance, the Chief of Defense Nuclear Security for NNSA elements, or the Director of Nuclear and National Security Information may cancel Secret or Confidential derivative classification authority when the employee's position no longer requires such authority or the employee cannot or does not exercise that authority reliably.
    - (a) By the Employee's Supervisor. The supervisor who cancels Secret or Confidential derivative classification authority for an employee under

his/her cognizance shall notify the employee and inform the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.

- (b) By the Designating Official. The designating official who cancels the Secret or Confidential derivative classification authority for an employee shall notify the employee and inform the employee's supervisor of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (c) By the Field Element Classification Officer. The Field Element Classification Officer who cancels the Secret or Confidential derivative classification authority for a contractor employee under his/her cognizance notifies the employee and informs the employee's supervisor and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (d) By the Chief of Defense Nuclear Security. Upon canceling the Secret or Confidential derivative classification authority for a contractor employee, the Chief of Defense Nuclear Security notifies the employee and informs the employee's supervisor and the designating official of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (e) By the Director of Nuclear and National Security Information. Upon canceling the Secret or Confidential derivative classification authority for a contractor employee, the Director of Nuclear and National Security Information notifies the employee and informs the employee's supervisor and the designating official (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the employee's name and position, the reason for cancellation, and the date the authority will end.
- f. Notification of Vacant Position. When an employee vacates a position that requires Top Secret derivative classification authority, the supervisor shall promptly inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA contractors) of the employee's name, position, and date of departure.

4. DERIVATIVE DECLASSIFIER. The Director of Nuclear and National Security Information designates specific individuals as Derivative Declassifiers. These individuals may exercise derivative declassification authority only while occupying those positions for which the authority was granted. This authority may not be assumed by an individual serving in an acting capacity. This authority is not retained when the individual transfers to another position. If an individual vacates a position that requires derivative declassification authority, the individual who will

permanently fill the vacancy is not automatically granted the authority, but is designated only in accordance with the procedures in Paragraph 4b below.

- a. Qualifications. To be nominated as a Derivative Declassifier, a contractor employee shall—
  - (1) have a scientific or technical degree (the Director of Nuclear and National Security Information may waive this requirement for nominees with suitable experience);
  - (2) have demonstrated competence in the subject area in which the authority will be used; and
  - (3) be familiar with DOE classification and declassification policy, procedures, and guidance, especially in the subject area for which the authority will be used.
  
- b. Designation Process.
  - (1) Request for Designation. The employee's supervisor or higher shall submit a designation request to the Director of Nuclear and National Security Information, through the appropriate contractor and field element Classification Officers (as well as through the Chief of Defense Nuclear Security for NNSA contractors). The Office of Nuclear and National Security Information (301-903-0368) can provide detailed instructions on how to submit the request.
  - (2) Evaluation of Request. The Director of Nuclear and National Security Information evaluates the need for the authority and the qualifications of the individual.
  - (3) Required Training.
    - (a) New Derivative Declassifier. Prior to being designated as a Derivative Declassifier, each employee shall successfully complete a training program and examination given by the Office of Nuclear and National Security Information. In addition, the local classification office shall provide training specific to the documents and material being reviewed for declassification.
    - (b) Derivative Declassifier Recertification. To recertify as a Derivative Declassifier, an employee shall successfully complete an examination given by the Office of Nuclear and National Security Information.
    - (c) Waiver of Required Training. The Director of Nuclear and National Security Information may waive the required training and examination

for an employee who has met the requirements within the last 3 years and who is transferring from a similar programmatic position.

- (4) Designation. The Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA contractors) designates in writing each Derivative Declassifier. Each designation identifies the organizations and specific subject areas covered by the Derivative Declassifier's authority and states the date the authority expires.
- c. Duration of Authority. Derivative declassification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.
- d. Redelegation. Derivative declassification authority cannot be redelegated.
- e. Cancellation of Authority. The employee's supervisor, the Chief of Defense Nuclear Security for NNSA contractors, or the Director of Nuclear and National Security Information may cancel derivative declassification authority when an employee's position no longer requires such authority or if the employee cannot or does not exercise that authority reliably.
- (1) By the Employee's Supervisor. The supervisor who cancels the derivative declassification authority for an employee under his/her cognizance shall notify the employee and inform the Director of Nuclear and National Security Information (as well as the Chief of Defense Nuclear Security for NNSA contractors), through the contractor and/or field element Classification Officer(s), of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (2) By the Chief of Defense Nuclear Security. Upon canceling the derivative declassification authority for an employee, the Chief of Defense Nuclear Security shall notify the employee and inform the employee's supervisor and the Director of Nuclear and National Security Information of the employee's name and position, the reason for cancellation, and the date the authority will end.
- (3) By Director of Nuclear and National Security Information. Upon canceling the derivative declassification authority for a contractor employee, the Director of Nuclear and National Security Information notifies the employee and informs the employee's supervisor, through the contractor and/or field element Classification Officer(s) (as well as the Chief of Defense Nuclear Security for NNSA contractors), of the employee's name and position, the reason for cancellation, and the date the authority will end.
- f. Notification of Vacant Position. When an employee vacates a position that requires derivative declassification authority, the contractor Classification Officer shall promptly inform the Director of Nuclear and National Security Information, through the

appropriate field element Classification Officer (as well as the Chief of Defense Nuclear Security for NNSA contractors), of the employee's name, position, and date of departure.

## PART B - ADMINISTRATIVE POLICIES

1. PERFORMANCE STANDARDS. The head of a contractor organization shall ensure that the management of classified information is included as a critical element or item to be evaluated in the performance standards of Classification Officers and any other individuals whose duties include significant involvement in generating classified information, documents, or material.
2. CHALLENGES TO CLASSIFICATION.
  - a. Restricted Data/Formerly Restricted Data.
    - (1) Challenge. An employee may formally challenge an RD/FRD classification determination with the Derivative Classifier who made the determination. Under no circumstances shall an individual be subject to retribution for such a challenge. The Derivative Classifier shall respond to the challenge within 90 calendar days. If no response is received, the employee may submit an initial appeal to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA contractors).
    - (2) Initial Appeal to Director of Nuclear and National Security Information. If the response by the Derivative Classifier does not satisfy the employee making the challenge, the employee may appeal the determination by writing to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA contractors), who is required to respond within 90 calendar days. If no response is received, the employee may submit a final appeal to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA contractors).
    - (3) Final Appeal to Director of Security Affairs. If the response by the Director of Nuclear and National Security Information does not satisfy the employee making the challenge, the employee may appeal the determination to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA contractors).
  - b. National Security Information.
    - (1) Challenge. An employee may formally challenge an NSI classification determination by writing to the Director of Nuclear and National Security Information (with a copy to the Chief of Defense Nuclear Security for NNSA contractors). The Director of Nuclear and National Security Information shall respond (with a copy to the Chief of Defense Nuclear Security for NNSA contractors) within 60 calendar days. Under no circumstances shall an individual be subject to retribution for such a challenge. If the Director is unable to respond within 60 calendar days, he/she acknowledges the challenge in

writing and provides a date when the employee can expect a response. If the Director of Nuclear and National Security Information has not responded to the challenge within 120 calendar days, the employee may forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP), as described in Appendix A to 32 CFR Part 2001.

- (2) Appeal to Director of Security Affairs. If the response by the Director of Nuclear and National Security Information does not satisfy the employee making the challenge, the employee may appeal the determination to the Director of Security Affairs (with a copy to the Chief of Defense Nuclear Security for NNSA contractors). The Director of Security Affairs shall respond (with a copy to the Chief of Defense Nuclear Security for NNSA contractors) within 90 calendar days. If the Director of Security Affairs has not responded to the appeal within 90 calendar days, the employee may forward the challenge to the ISCAP, as described in Appendix A to 32 CFR Part 2001.

3. REPORTING REQUIREMENTS. Each contractor Classification Officer shall compile statistics requested by the Office of Nuclear and National Security Information and provide them to the Director of Nuclear and National Security Information, through the appropriate field element Classification Officer and the Chief of Defense Nuclear Information for NNSA contractors, for use in assessing DOE success at meeting performance measurements and for inclusion in reports required by the Information Security Oversight Office and 10 CFR Part 1045.
4. MISCLASSIFICATION OF INFORMATION, DOCUMENTS, OR MATERIAL.
- a. Deliberate Action. Any knowing or willful action that results in the misclassification of information, documents, or material violates the requirements in this CRD and may result in criminal, civil, and/or administrative penalties. Such an action may also result in a security infraction or violation, as covered under DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, and DOE O 471.2A, INFORMATION SECURITY PROGRAM. However, security infractions are not intended to be issued in cases where classifiers disagree for legitimate reasons. Examples of situations in which security infractions will be issued include classifying with no authority and classifying outside of granted authority.
- b. Negligence in Exercising Classification/Declassification Authority. The appropriate official (as indicated in Part A of this chapter) shall promptly cancel the classification authority of any individual who demonstrates gross negligence or a pattern of negligence or carelessness in applying the requirements in this CRD that results in the misclassification of information, documents, or material.
5. DEVIATIONS FROM REQUIREMENTS. A contractor Classification Officer may propose an alternate or equivalent means of meeting a specific requirement in this CRD or he/she may

request an exemption. Such a proposal shall describe the variance or waiver and explain why it is needed. The proposal shall be submitted to the Director of Nuclear and National Security Information through the field element Classification Officer or Headquarters Classification Representative and Chief of Defense Nuclear Security for NNSA contractors for approval (required within 30 days). Each approved deviation shall be examined during an oversight review to ensure it is still needed.

## CHAPTER II

### CLASSIFICATION CATEGORIES AND LEVELS

#### 1. CATEGORIES OF CLASSIFIED INFORMATION.

##### a. Restricted Data and Formerly Restricted Data.

(1) Restricted Data. Information classified under the Atomic Energy Act that concerns—

- (a) the design, manufacture, or utilization of nuclear weapons;
- (b) the production of special nuclear material; or
- (c) the use of special nuclear material in the production of energy.

RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.

(2) Formerly Restricted Data. Information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.

b. National Security Information. Information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

#### 2. LEVELS OF CLASSIFICATION. The following levels of classification, listed in descending order of sensitivity, may be applied to RD, FRD, or NSI:

- a. Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.
- b. Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- c. Confidential. The damage tests for RD/FRD and NSI are different, as noted below:

- (1) Restricted Data/Formerly Restricted Data. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - (2) National Security Information. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.
3. USE OF THE TERM "UNCLASSIFIED." The term "Unclassified" is used to identify information that is not classified under a statute or Executive order. Unclassified information is not normally marked as "Unclassified" except to distinguish it from classified information and then only when such distinction is required or otherwise serves a useful purpose. The fact that information is unclassified does not mean that it may be released to the public.

## CHAPTER III

### CLASSIFYING AND DECLASSIFYING INFORMATION

Classifying and declassifying information as RD, FRD, or NSI is a function performed by Federal Government officials only. However, the following areas are relevant to contractor employees:

1. Request for Determination. An employee who develops a new, nuclear-related subject area that he/she believes may be classified shall request an evaluation of the subject area by the Director of Nuclear and National Security Information, through the appropriate contractor and field element Classification Officers and with a copy to the Chief of Defense Nuclear Security for NNSA contractors. The Director of Nuclear and National Security Information is required to make a determination within 90 calendar days.
2. Unauthorized Disclosure. Information classified as RD, FRD, or NSI is not declassified automatically because of any unauthorized disclosure of identical or similar information.
3. Declassification Proposals.
  - a.. Ad Hoc Proposals. At any time, contractor employees may submit proposals for declassifying information to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA contractors) for evaluation. Such proposals may be submitted to achieve a variety of goals, such as challenging classification policy, reducing operating costs, and transferring technology to the private sector.
  - b. Disposition of Proposal. The Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA contractors) notifies the contractor employee making a proposal of its disposition within 1 month after the final determination.

## CHAPTER IV

### CLASSIFICATION GUIDANCE

#### 1. GENERAL.

- a. Purpose. Classification guidance contains detailed instructions for determining whether specific information is classified or unclassified. Examples of guidance include—but are not limited to—program guides, topical guides, local guides, bulletins, and change notices.
- b. Content. At a minimum, classification guidance identifies elements of information that are classified or unclassified in a specific area. For the classified information, the guidance prescribes the classification level and category. For information classified as NSI, the guidance also states a concise reason for classifying the information and prescribes declassification instructions or the category for exemption from automatic declassification for each element of information.
- c. Inconsistent Guidance. Guidance may be inconsistent for three reasons; each reason requires a different course of action.
  - (1) Ambiguous Guidance. When information is described equally well by more than one topic but uncertainty exists about which topic applies, the most restrictive guidance shall apply until clarification is obtained.
  - (2) Outdated Guidance. Due to difficulties in revising all guidance simultaneously to reflect declassification actions, some guidance may specify different classifications for the same information. The guidance with the most current date shall apply.
  - (3) Conflicting Guidance. When the same information is classified differently in separate guidance and neither appears to be more current or authoritative than the other, the most restrictive guidance shall apply until clarification is obtained.
- d. No Guidance. A Derivative Classifier or Derivative Declassifier who cannot determine the proper classification of an element of information using classification guidance approved for his/her use shall contact the local Classification Officer for assistance. Local Classification Officers who cannot provide assistance shall refer the issue through the field element Classification Officer (with a copy to the Chief of Defense Nuclear Security for NNSA contractors) to the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information is required to make a classification determination within 90 calendar days. Pending this final determination, the document or material containing the information in question shall be marked and protected according to DOE M 471.2-1A, MANUAL FOR

CLASSIFIED MATTER PROTECTION AND CONTROL, issued by the Office of Safeguards and Security.

2. TYPES OF GUIDANCE.

a. Headquarters Guidance.

- (1) Purpose. Headquarters guidance contains detailed classification and declassification instructions in one or more subject areas.
- (2) Originator/Approval Authority. Headquarters guidance covering only DOE information is developed, approved, and issued by the Director of Nuclear and National Security Information. Headquarters guidance covering information for which DOE and other Government agencies or foreign countries are responsible (known as joint guidance) is approved and issued by the Director of Nuclear and National Security Information in coordination with officials from the other Government agencies or foreign countries involved. Headquarters guidance shall name its approving official(s) and indicate the approval date.
- (3) Basis. Headquarters guidance is based on classification and declassification determinations made by the Directors of Nuclear and National Security Information and Security Affairs.
- (4) Users. Derivative Classifiers and Derivative Declassifiers use Headquarters guidance as the basis for derivative determinations; however, they may use only that guidance pertaining to the specific subject areas described in their designations of authority. A local classification office may also use Headquarters guidance to prepare detailed local guidance intended primarily for use within the field element or contractor organization.

b. Local Guidance.

- (1) Purpose. Local guidance has the same purpose as Headquarters guidance, but is more detailed and is tailored to the specific needs of the originating field element or contractor organization. If existing Headquarters guidance is adequate for the needs of the organization, local guidance is not required. If proposed local guidance affects DOE or contractor elements other than the issuing organization, a Government agency other than DOE (such as the Department of Defense), or a foreign government, the Director of Nuclear and National Security Information shall issue Headquarters guidance to cover the information.
- (2) Originator/Approval Authority. The local classification office may issue local guidance following approval by the Director of Nuclear and National Security Information. The Director of Nuclear and National Security Information may

delegate approval authority in writing to field element Classification Officers on a case-by-case basis. Local guidance shall name its approving official and indicate the approval date.

- (3) Basis. Local guidance is based on Headquarters guidance.
- (4) Users. Derivative Classifiers and Derivative Declassifiers shall use local guidance as the basis for derivative determinations; however, they may use only that guidance pertaining to the specific subject areas described in their designations of authority. Unless otherwise directed by the Director of Nuclear and National Security Information, local guidance may be disseminated to other organizations, both inside and outside DOE, providing each organization has a need to know and facility clearance at the appropriate classification level.
- (5) Copies of the Local Guidance. Within 10 calendar days of approval, any organization that issues local guidance shall send a disk containing the entire text of the guidance in either ASCII or WordPerfect (version 5.1 or higher) format and five copies of the issued guidance to the Director, Technical Guidance Division, Office of Nuclear and National Security Information.

### 3. RELATED POLICIES AND PROCEDURES.

#### a. Updating Guidance.

- (1) Erroneous Guidance. Each issuing organization that learns its guidance contradicts current policy shall distribute revised guidance within 120 calendar days.
- (2) Periodic Review of Classification Guidance. Each organization that issues guidance shall maintain a list of its guidance and shall review and update such guidance as changes in classification policy are received (or in any event, at least once every 5 years) to ensure consistency with DOE classification policy. If the guidance is consistent with policy, the reviewer shall annotate the record copy of the guidance with the results and date of the review. If the guidance contradicts policy, the issuing organization shall revise the guidance and distribute it within 120 calendar days. Completion of this review does not require a specific report to the Director of Nuclear and National Security Information, but oversight reviews shall include an examination of these records of guidance review.
- (3) Distributing New or Revised Headquarters Guidance. Each Classification Officer shall distribute new or revised Headquarters guidance to appropriate classifiers and declassifiers within 30 calendar days of receiving it. However, if the new or revised Headquarters guidance affects local guidance, the

Classification Officer shall revise and distribute the local guidance within 120 calendar days.

- b. Classification Guidance for DOE Contractors.
- (1) Identification of Required Classification Guidance. Each procurement request originator determines if a proposed contract may generate classified information. If it does, the procurement request originator shall complete Block 10 on DOE Form 5634.2, "Contract Security Classification Specification," which identifies classification guidance that will apply to the proposed contract. If necessary, the procurement request originator may request assistance from the cognizant classification office to identify the appropriate classification guidance.
  - (2) Approval of Classification Guidance. The Classification Officer shall sign Block 15 of DOE Form 5634.2 for any subcontracts awarded to certify that the classification guidance being provided is appropriate for the work to be performed. This authority may be delegated in writing to specific Derivative Classifiers in the Classification Officer's organization. With the concurrence of the Director of Nuclear and National Security Information, the Classification Officer may also delegate this authority to a technically competent Derivative Classifier outside his/her staff.
- c. Classification Guidance for Non-DOE, Including non-NNSA, Funded Work. Non-DOE, including non-NNSA, funded work that may generate classified information is conducted in accordance with DOE O 481.1, WORK FOR OTHERS (NON-DOE FUNDED WORK), and accompanying CRD, and classification guidance is issued by the funding organization. For unclassified work, the funding organization shall provide a written statement that classified activities are not part of the project.
- (1) Certification of Guidance. The Classification Officer under whose purview the work will be conducted shall review the work request and the proposed classification guidance. He/she shall use DOE Form 5634.2, Department of Defense Form DD-254, "Contract Security Classification Specification," or any other form provided by the funding organization to certify that the guidance is adequate and does not contradict DOE policy. The Classification Officer may delegate the authority to review and certify classification guidance to a member of his/her staff. With the concurrence of the Director of Nuclear and National Security Information, the Classification Officer may also delegate this authority to a technically competent Derivative Classifier outside his/her staff.
  - (2) Additional Guidance Required. If additional guidance is required, DOE, including NNSA, the sponsoring agency, or both may develop the guidance, and the sponsoring agency shall approve it.

## CHAPTER V

### CLASSIFYING AND DECLASSIFYING DOCUMENTS AND MATERIAL

#### PART A - CLASSIFICATION

Heads of the contractor organizations shall ensure that documents and material prepared under their purview are reviewed and processed in accordance with the provisions of this part.

1. **AUTHORITY.** A Derivative Classifier may derivatively classify a document or material containing RD, FRD, and/or NSI only within his/her programmatic jurisdiction at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority.
  - a. **Restricted Data/Formerly Restricted Data.** A Derivative Classifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the classifier's designation of authority. If no guidance exists, refer to Chapter IV, Paragraph 1d.
  - b. **National Security Information.** A Derivative Classifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the classifier's designation of authority. If no guidance exists, refer to Chapter IV, Paragraph 1d. However, when information is extracted from a classified document, that document can be cited as a basis for classification if the information is entirely under the purview of another Government agency, a foreign government, or an international organization, and no joint classification guidance exists.
2. **REVIEW REQUIREMENTS.** Anyone who originates a document or material in a subject area that may be classified shall submit the document or material to the appropriate official for a classification review and determination prior to dissemination.
  - a. **Current Employee.**
    - (1) **Possesses an Active Access Authorization or Had One in the Past.**
      - (a) **Routine Document or Material.** An employee with an active access authorization who originates a document or material in a subject area that may be classified shall submit the document or material to a Derivative Classifier for classification review prior to dissemination. An employee who had an active access authorization in the past shall submit such a document or material to the local Classification Officer for classification review prior to dissemination. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.

- (b) Public Release or Widespread Distribution. A document or material that is prepared in a potentially classified subject area may be intended for public release or have such widespread internal distribution that public release is likely. In such cases, the originator shall submit the document or material to the local Classification Officer for classification review prior to dissemination. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
  - (c) Oral Presentations. An employee who is making an oral presentation in a subject area that may be classified shall submit the prepared text to the local Classification Officer for classification review prior to making the presentation. This includes any presentation made to the public as well as any presentation made to a sufficiently large, internal audience in an unclassified setting, making public release of the information likely. If the employee does not have a prepared text or if extemporaneous remarks are likely, the local Classification Officer shall brief the employee on classification guidance pertinent to the subject matter, including related topics the employee should avoid because they may be classified. The local Classification Officer may delegate this review and briefing responsibility to specified Derivative Classifiers.
- (2) Never Had an Access Authorization. An employee who has never had an access authorization may originate a document or material in a subject area that may be classified. In such cases, the local Classification Officer shall review the document or material for classification prior to dissemination. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
- b. Not an Employee.
- (1) Possesses an Active Access Authorization. The local Classification Officer shall review for classification a document or material that is submitted by an individual who is not employed by the contractor but possesses an active access authorization. The local Classification Officer may delegate this review responsibility to specified Derivative Classifiers.
  - (2) Had an Access Authorization in the Past or Never Had an Access Authorization. The local Classification Officer shall forward to the Director of Nuclear and National Security Information any document or material that is submitted for classification review by an individual who is not employed by the contractor but had an access authorization in the past or has never had an access authorization.
3. REQUIRED MARKINGS. The Derivative Classifier shall ensure the following markings are included on the document or material being derivatively classified (see DOE M 471.2-1A,

MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL, for complete information on marking requirements).

a. Restricted Data/Formerly Restricted Data.

- (1) Overall classification level and category of the document.
- (2) Classification level and category of each interior page of the document if not using the overall classification level and category on each page.
- (3) Classification authority (i.e., "Classified By:").
  - (a) Name or personal identifier of the Derivative Classifier.
  - (b) Position title of the Derivative Classifier.
- (4) Designation of the guidance or source document(s) used to make the classification determination and the date of such document(s) (i.e., "Derived From").

b. National Security Information.

- (1) Overall classification level of the document.
- (2) Classification level of each interior page of the document if not using the overall classification level on each page.
- (3) Portion marking for each section, part, paragraph, graphic, figure, or similar portion (for documents containing NSI only).
- (4) Classification authority (i.e., "Classified By").
  - (a) Name or personal identifier of the Derivative Classifier.
  - (b) Position title of the Derivative Classifier.
- (5) Designation of the guidance or source document(s) used to make the classification determination and date of such document(s) (i.e., "Derived From").
- (6) Duration of classification derived from the guidance or source document(s) (i.e., "Declassify On").
  - (a) Date - A specific date 10 years or less from the date of the document or as specified by the guidance or source document(s).

- (b) Event - A specific event occurring less than 10 years from the date of the document as specified by the guidance or source document(s).
  - (c) Exempt from declassification - Document is exempt from declassification at 10 years and identified by an exemption category (e.g., X1 through X8) as specified by the guidance or source document(s).
  - (d) Extension of classification - Classification of the document may be extended for successive periods not to exceed 10 years at a time. The "Declassify On" line shall be revised to include the date of the extension action, the new declassification date, and the person authorizing the extension.
  - (e) Reclassification - As appropriate, a document may be reclassified. The "Declassify On" line shall be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.
- c. Mixed Document. A mixed document contains both Restricted Data/Formerly Restricted Data information and National Security Information.
- (1) Overall classification level and category of the document (RD/FRD information takes precedence over NSI).
  - (2) Classification level and category (if RD or FRD) of each interior page of the document if not using the overall classification level and category on each page.
  - (3) Classification authority (i.e., "Classified By").
    - (a) Name or personal identifier of the Derivative Classifier.
    - (b) Position title of the Derivative Classifier.
  - (4) Designation of the guidance or source document(s) used to make the classification determination and the date of such document(s) (i.e., "Derived From").
4. PORTION MARKING REQUIREMENTS. NOTE: Derivative Classifiers and Declassifiers shall base their determinations on classification guidance pertaining to the specific subject areas described in their designations of authority. If no guidance exists, they should refer to Chapter IV, Paragraph 1d.
- a. Restricted Data/Formerly Restricted Data Documents. Documents containing only RD/FRD should not be portion-marked.

- b. National Security Information Documents. Documents containing only NSI shall be portion-marked.
  - c. Mixed Documents. Documents or material containing both RD/FRD and NSI should not be portion-marked.
  - d. Documents Prepared Under Work-for-Others Contracts. Documents prepared under Work-for-Others contracts shall be portion-marked according to the rules stated in Paragraphs 4a through 4c above.
5. NOTIFICATION OF CLASSIFICATION. The Derivative Classifier who classifies a document shall notify the originator and provide sufficient information for the originator to identify the specific document being classified.
6. PROCEDURES RELATED TO THE REVIEW OF DOCUMENTS OR MATERIAL FOR CLASSIFICATION.
- a. Foreign Government Information. For additional information on marking documents containing foreign government information, refer to DOE M 471.2-1A, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
    - (1) Document or Material Generated by a Foreign Government. Review by a Derivative Classifier is not required to apply—
      - (a) a U.S. classification level that provides at least an equivalent level of protection to a document or material classified by the foreign government or
      - (b) the “Confidential—Modified Handling Authorized” marking to a document or material that the foreign government protects at a level lower than U.S. Confidential.
    - (2) Document or Material Generated by the United States. Review by a Derivative Classifier is required for a newly generated document or material concerning foreign government information that may also contain U.S. classified information.
  - b. Use of a Classified Addendum. To the maximum extent practical, the originator of a document containing classified information shall include the unclassified portions in the primary document and shall separate the classified portions into attachments, appendixes, or supporting documents. If such separation is not practical and there is significant public interest in the document, the originator is encouraged to prepare an unclassified version.

- c. External Coordination Reviews. A document or material being reviewed for classification may contain information under the cognizance of another Government agency or a foreign country. If the Derivative Classifier thinks the information may be classified and no guidance is available, he/she shall send the document or material to the local Classification Officer for further review or referral to the Director of Nuclear and National Security Information, through the field element Classification Officer.
  
- d. Classification Following Request for a Previously Unclassified Document. The public may request documents under a statute, Executive order, or regulation. Some of these documents may contain classified information, even if they are not so marked. Such documents shall be referred to the Director of Nuclear and National Security Information through the appropriate contractor and field element Classification Officers for review.

## PART B - DECLASSIFICATION

Heads of contractor organizations shall ensure that documents and material prepared under their purview are reviewed and processed in accordance with the provisions of this part.

1. **AUTHORITY.** A Derivative Declassifier may derivatively declassify a document or material originated in only those organizations and subject areas for which he/she has been delegated such authority and is governed by other limitations specified in the written designation. A Derivative Declassifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the declassifier's designation of authority. If no guidance exists, Derivative Declassifiers should refer to Chapter IV, Paragraph 1d.
2. **REVIEW REQUIREMENTS FOR REDACTING A DOCUMENT OR DECLASSIFYING A DOCUMENT OR MATERIAL.** Preparing a redacted version of a document (i.e., a version of the document with all classified information removed) or declassifying a document or material in full requires two reviews by individuals who are knowledgeable in the subject area. The first review may be conducted by either a Derivative Classifier or Declassifier. The second review shall be conducted by a Derivative Declassifier (other than the first reviewer), who shall confirm that all classified information has been identified and bracketed in the document to be redacted or that the declassified document or material is unclassified.
3. **REQUIRED MARKINGS.** For each document or material that is declassified, the Derivative Declassifier shall ensure that the following markings are included on the document or material and that the classification markings are crossed out:
  - a. date of declassification (i.e., "Declassified On");
  - b. name(s) and position(s) or title(s) of individual(s) declassifying the document (i.e., "Declassified By");
  - c. designation of the guidance or source document(s) used as the basis for the declassification determination and the date of such document(s) (i.e., "Derived From").
4. **DURATION OF CLASSIFICATION.**
  - a. **Restricted Data/Formerly Restricted Data.** Documents or material containing RD/FRD are never automatically declassified. Such documents or material remain classified until an authorized person takes positive action to declassify them. Under the Atomic Energy Act, no date or event for automatic declassification ever applies to RD/FRD documents or material, even if such documents or material also contain NSI.
  - b. **National Security Information.** DOE documents marked as containing NSI that do not specify a date or event for declassification are never automatically declassified. Section 3155(a) of Public Law 104-106 states that before such a document can be released or

declassified, it shall be reviewed to determine if it contains RD/FRD. If the document contains RD/FRD, it shall be so marked and may only be declassified under the provisions in Paragraph 4a above. However, if the document is determined to contain only NSI, the following paragraphs apply:

- (1) Marked with Specific Date or Event for Declassification. A document marked with a specific date or event for declassification is declassified after the date or event has passed. Anyone may remove or obliterate the classification markings on such a document.
- (2) Exemption from Declassification within 10 Years. A document marked as exempt from declassification within 10 years is not automatically declassified. Procedures for declassifying such a document are contained in Part B, Paragraph 2, above.
- (3) Historical Records.
  - (a) Permanent Records. If a document contains only NSI, is more than 25 years old, and has been determined to be a permanent record under Title 44 of the United States Code, a Derivative Declassifier shall determine if the document can be declassified or if it is exempt from the automatic declassification requirements based on guidance in the Historical Records Declassification Guide.
  - (b) Temporary and Unscheduled Records. A document that contains only NSI, is more than 25 years old, and has been determined to be a temporary record or is an unscheduled record is not subject to the automatic declassification requirements in this paragraph (i.e., Paragraph 4). Such a document retains its current classification status until it is reviewed using current classification guidance and determined to be unclassified under procedures in Paragraph 2 above. (NOTE: Unscheduled records have not been determined to be either permanent or temporary.)

## 5. TYPES OF DOCUMENT REVIEWS.

- a. Mandatory Review Requests. Any contractor employee who receives a mandatory review request for a document containing RD/FRD information or NSI shall send the request to the Director of Nuclear and National Security Information through the appropriate contractor and field element Classification Officers for processing.
- b. Systematic Reviews.
  - (1) Restricted Data/Formerly Restricted Data. The local classification office shall ensure that documents containing RD/FRD information are periodically and

systematically reviewed for declassification. Such reviews shall be based on the degree of public and researcher interest and the likelihood of declassification upon review.

(2) National Security Information. The local classification office shall ensure that documents containing NSI that have been exempted from automatic declassification are periodically and systematically reviewed for declassification. Such reviews shall be based on the degree of public and researcher interest and the likelihood of declassification upon review.

c. Other Reviews. The local classification office shall ensure that documents or material containing RD/FRD information or NSI are reviewed for declassification for any reason other than those defined in Paragraphs 5a and 5b above (e.g., congressional testimony, litigation, and reviews to preclude erroneous automatic declassification).

## 6. DOCUMENT REVIEW PLAN.

a. Determining Need for a Plan. The contractor Classification Officer shall notify the Director of Nuclear and National Security Information through the appropriate field element Classification Officer and the Chief of Defense Nuclear Security for NNSA elements whenever a group of documents to be reviewed for declassification exceeds 10,000 pages. Such notification shall describe why the review is necessary, estimate the number of pages or volume of material requiring review, and describe the anticipated impact on resources. After consulting with the contractor Classification Officer, the Director of Nuclear and National Security Information shall determine if the contractor Classification Officer needs to develop a document review plan.

b. Contents of the Plan. The plan shall-

- (1) describe why the review is required;
- (2) contain detailed, written procedures that describe how the technical and administrative aspects of the review will be conducted;
- (3) contain a statistically valid quality assurance assessment plan with standards for remedial action specified;
- (4) summarize exceptions and deviations from standards;
- (5) provide the names and classification/declassification authorities of the reviewers;
- (6) list the classification guidance to be used; and
- (7) contain a sample of the stamps to be used.

- c. Submission and Approval of the Plan. The contractor Classification Officer shall submit the plan to the Director of Nuclear and National Security Information, through the appropriate field element Classification Officer and the Chief of Defense Nuclear Security for NNSA elements, for approval prior to starting work.
7. NOTIFICATION OF DECLASSIFICATION. For documents less than 25 years old, the Derivative Declassifier who declassifies a document shall notify the originator or document custodian to the maximum extent possible and provide sufficient information for the originator or document custodian to identify the specific document being declassified.
8. PROCEDURES RELATED TO THE DECLASSIFICATION REVIEW OF DOCUMENTS OR MATERIAL.
  - a. Public Release. Declassifying a document or material does not mean that it may be released to the public automatically. Information contained in the document or material may still be exempt from release for other reasons; therefore, once a document or material is declassified, it must still be reviewed to determine if the information falls within any of the Freedom of Information Act exemptions before it can be released to the public.
  - b. External Coordination Reviews.
    - (1) DOE, including NNSA, Documents or Material. Prior to declassifying a document or material containing information under the cognizance of another DOE, including NNSA, element, a Derivative Declassifier shall either send the document or material to that organization for review or obtain the concurrence of that organization that the document or material can be declassified unless specific authority to declassify the document or material has been delegated.
    - (2) Other Agency Documents. The Director of Nuclear and National Security Information conducts any interagency coordination required to declassify a document or material containing RD/FRD information or NSI when the document or material relates to litigation or has been requested under the Freedom of Information Act. In all other cases, contractor Classification Officers shall conduct any interagency coordination required to declassify a document or material containing either RD/FRD information or NSI. To assist with this coordination, the Office of Nuclear and National Security Information provides contractor Classification Officers with the names and addresses of appropriate interagency points of contact.
    - (3) Foreign Government and International Organization Documents or Material. Unless public release is specifically authorized through current classification guidance, the Director of Nuclear and National Security Information conducts all coordination required to declassify a document or material that contains information-

- (a) provided to the United States by a foreign government or international organization or
  - (b) produced by the United States under a joint arrangement with a foreign government or international organization.
- c. OpenNet Data Base. Each contractor that declassifies a document and determines that it may be released to the public shall ensure that the following information is submitted to the Office of Scientific and Technical Information for inclusion on the OpenNet data base:
  - (1) a bibliographic reference to the document and
  - (2) the location where the document is available to the public.
- d. Obsolete Classification Markings. Documents dated prior to December 15, 1953, and marked as "Restricted" and documents dated between July 18, 1949, through October 22, 1951, and marked as "Official Use Only" were considered classified. However, markings are either no longer used or have a different meaning.
  - (1) Review Requirements. A Derivative Classifier or Declassifier (only one review is required) shall review such documents to determine their current classification status. Until that review is completed, the documents shall be marked and protected according to DOE M 471.2-1A, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.
  - (2) Determined to be Classified. If a Derivative Classifier determines the documents are classified, the "Restricted" or "Official Use Only" markings shall be crossed out and replaced with current classification markings. The Derivative Classifier shall prepare an upgrading notice, as appropriate.
  - (3) Determined Not to be Classified. If a Derivative Classifier or Declassifier determines the documents are not classified, the "Restricted" or "Official Use Only" markings shall be crossed out and replaced with the marking "Unclassified," along with the name of the reviewer. A declassification notice is not required.
- e. Extracted Version of Document. A major portion of an existing classified document (i.e., a chapter or appendix) may be extracted for use as a new document. Such a document shall be clearly identified as an extract and shall be marked and protected according to DOE M 471.2-1A, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL. A Derivative Classifier shall review the new document to determine if it contains classified information.

- f. Redacted Version of Document. A redacted document shall clearly indicate it is a redacted version.
  
- g. Review Upon Termination of Employment. A contractor employee who retires or otherwise terminates employment may wish to take correspondence, personal records, diaries, or other documents with him/her. If these records fall wholly or partially in areas that are classified, a review by a Derivative Classifier is required.

## PART C - DOWNGRADING OR UPGRADING

### 1. GENERAL.

- a. Downgrading occurs when an appropriate authority determines the document or material can be adequately protected at a classification level or category lower than currently marked, not including "Unclassified." (Downgrading to "Unclassified" is called declassifying, which is covered under Part B of this chapter.)
- b. Upgrading occurs when an appropriate authority--
  - (1) assigns the appropriate classification level and/or category to a document or material erroneously issued as unclassified or
  - (2) raises the classification level or category of a document or material to protect the contents adequately.

### 2. AUTHORITY.

- a. Downgrading. A Derivative Declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of notice from the proper authority.
- b. Upgrading. A Derivative Classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of notice from the proper authority.

### 3. NOTIFICATION OF DOWNGRADING OR UPGRADING.

- a. Downgrading. The Derivative Declassifier authorizing the downgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being downgraded.
- b. Upgrading. The Derivative Classifier authorizing the upgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being upgraded. The Derivative Classifier shall refer to appropriate classification guidance when preparing upgrading notices because such notices may be classified.

## PART D - RECLASSIFICATION

1. AUTHORITY.
  - a. General. A Derivative Classifier may reclassify a document or material within his/her designated authority.
  - b. Following Request for a Previously Declassified Document. The public may request declassified documents under a statute or Executive order. Some of these documents may inadvertently still contain classified information. Such documents shall be referred to the Nuclear and National Security Information, through the appropriate contractor and field element Classification officers and the Chief of Defense Nuclear Security for NNSA elements, for review.
2. NOTIFICATION OF RECLASSIFICATION. The Derivative Classifier authorizing the reclassification of a document or material shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document or material being reclassified. The Derivative Classifier shall refer to appropriate classification guidance when preparing a reclassification notice because such notices are usually classified.

## CHAPTER VI

### EDUCATION PROGRAM

1. INITIAL CLASSIFICATION EDUCATION. All cleared DOE, including NNSA, contractor employees must understand their classification/declassification responsibilities. Each contractor Classification Officer shall ensure that such employees receive a classification orientation that includes identification of a point of contact to answer questions or address concerns about classification or declassification matters.
2. CONTINUING EDUCATION. Each contractor Classification Officer shall ensure that a continuing classification education program is conducted annually for all cleared employees to maintain classification awareness and inform them of applicable changes in classification policies, principles, guidance, and procedures.
3. INITIAL TRAINING FOR A CLASSIFIER OR DECLASSIFIER. Before becoming Derivative Classifiers or Derivative Declassifiers, individuals shall receive training covering the following elements and shall successfully complete an examination to ensure they understand these elements sufficiently:
  - a. Derivative Classifier:
    - (1) the process of original and derivative classification and the standards applicable to each,
    - (2) the markings that must appear on a derivatively classified document, and
    - (3) the authorities, methods, and processes for downgrading and declassifying information, documents, and material.
  - b. Derivative Declassifier:
    - (1) the standards, methods, and procedures for declassifying documents or material under the Atomic Energy Act and Executive Order 12958,
    - (2) the standards for using declassification guidance,
    - (3) the markings that must appear on a derivatively declassified document,
    - (4) the contents of the DOE declassification plan, and
    - (5) DOE responsibilities for establishing and maintaining a declassification data base.
4. RECERTIFICATION TRAINING. To recertify as a Derivative Classifier or Derivative Declassifier, an individual shall successfully complete an examination that, at a minimum, retests his/her understanding of applicable classification and declassification policies, principles, procedures, and guidance.

## CHAPTER VII

### CLASSIFICATION AND DECLASSIFICATION OVERSIGHT PROGRAM

1. **PERFORMANCE OBJECTIVE.** The Office of Nuclear and National Security Information manages the classification and declassification oversight program that ensures that all contractor and subcontractor organizations that generate classified information and documents or material have implemented and maintain an adequate and effective classification and declassification program.
2. **SCOPE.**
  - a. **Differing Scope and Complexity.** Classification and declassification programs at various contractor facilities differ in scope and complexity. No single list of areas to be covered in an oversight review is appropriate in all cases. Therefore, the scope of the oversight review must be tailored to ensure that it provides the management and oversight necessary to evaluate the adequacy and effectiveness of each individual classification and declassification program.
  - b. **Uniformity of Oversight Reviews.** To introduce a measure of uniformity into classification and declassification oversight reviews, each review shall cover, at a minimum, the following areas:
    - (1) management awareness and support,
    - (2) document reviews,
    - (3) guidance,
    - (4) education,
    - (5) classifiers and declassifiers,
    - (6) declassification,
    - (7) effectiveness of the program to publicly release declassified documents, and
    - (8) oversight reviews of subcontractors.
3. **FREQUENCY OF OVERSIGHT REVIEWS.** The frequency of oversight reviews is determined after considering the following factors:
  - a. **Past Performance Experience and Review Results.** More frequent reviews are conducted of facilities that have experienced problems previously.

- b. Interval Since Last Review. Facilities having a major classification and declassification interest are reviewed every 2 years unless particular circumstances indicate otherwise. Facilities with effective classification and declassification programs or minor interests may be reviewed less frequently (every 3-5 years). The local Classification Officer shall determine the frequency of oversight reviews of subordinate facilities.
4. OVERSIGHT REVIEW REPORTS. The oversight review report shall ensure the organization reviewed receives a clear explanation of its performance. The review report shall ensure that deficiencies or problem areas are identified.
5. FOLLOW-UP MEASURES. Follow-up measures shall ensure that the actions taken to correct deficiencies noted during an oversight review are adequate and have been implemented in a timely manner.
6. SELF-ASSESSMENTS. Each contractor organization that generates classified information and documents or material shall establish and maintain an ongoing self-assessment program, documented in writing to the appropriate field element Classification Officer. Self-assessments shall be conducted annually unless prior agreement is reached with the field element Classification Officer.

## CHAPTER VIII

### DEFINITIONS

1. Automatic Declassification. The declassification of a document or material based solely upon the occurrence of a specific date or event as determined by classification guidance or the expiration of a maximum time frame for duration of classification established under Executive Order 12958.
2. Classification Guidance. A written record of detailed instructions as to whether specific information is classified, usually concerning a system, plan, project, or program. The guidance identifies information to be classified and specifies the level (and duration for National Security Information only) of classification assigned to such information. Classification guidance is the primary basis for reviewing documents or material to determine whether they contain classified information.
3. Classification Officer.
  - a. Headquarters Classification Officer. The Nuclear and National Security Information.
  - b. Field Element Classification Officer. An individual designated to administer the classification program for that particular field element and to monitor the classification programs of contractors under its cognizance.
  - c. Contractor Classification Officer. An individual designated to administer the classification program for that particular contractor and to monitor the classification programs of subcontractors under its cognizance.
  - d. Local Classification Officer. For DOE and NNSA Headquarters elements, the Nuclear and National Security Information is the local Classification Officer. For field elements with no designated Classification Officer, the Nuclear and National Security Information is the local Classification Officer. For contractors with no designated Classification Officer, the appropriate field element Classification Officer is the local Classification Officer.
4. Classified Information. Information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, as amended, or information determined to require protection against unauthorized disclosure under Executive Order 12958 or prior Executive orders, which is identified as National Security Information.
5. Declassification. A determination by an appropriate authority that information or documents and material no longer require protection as classified information against unauthorized disclosure because of national security concerns.

6. Denying Official. An individual, designated under 10 CFR Part 1004, who is authorized to make the final decision on what information contained in a document requested under the Freedom of Information Act may be withheld.
7. Derivative Classification. A determination based on classification guidance or source documents that a document or material contains Restricted Data, Formerly Restricted Data, and/or National Security Information.
8. Derivative Classifier. An individual authorized to determine that a document or material is unclassified or classified as Restricted Data, Formerly Restricted Data, and/or National Security Information and at what level based on classification guidance or source documents. (A Derivative Classifier is equivalent to the Restricted Data Classifier referred to in 10 CFR Part 1045.)
9. Derivative Declassifier. An individual authorized to declassify or downgrade documents or material in specified areas based on classification or declassification guidance or source documents.
10. Document. Written or printed information; removable ADP media (diskettes, tapes, cards, etc); charts; maps; paintings; drawings; engravings; sketches; photographic prints; exposed or developed film; working notes and papers; reproductions of such things by any means or process; and sound and video recordings generated by magnetic, optical, or any other electronic means.
11. Downgrading. A determination by an appropriate authority that (a) information may be handled at a level lower than the initial classification level or (b) a document or material may be handled at a level and/or category lower than the initial classification level and/or category. In either case, however, the revised classification level shall not be lower than Confidential.
12. Foreign Government Information. Such information consists of one of the following:
  - a. information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
  - b. information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
  - c. information received and treated as "Foreign Government Information" under the terms of a predecessor order.

13. Formerly Restricted Data (FRD). Classified information jointly determined by the Director of Security Affairs and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the Director of Security Affairs from the Restricted Data category pursuant to Section 142(d) of the Atomic Energy Act, as amended, and safeguarded as National Security Information, subject to restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.
14. Headquarters Classification Representative. An individual designated by his/her Headquarters element to serve as the point of contact with the Office of Nuclear and National Security Information on classification and declassification policies and procedures and to assist others in his/her Headquarters element with their classification and declassification responsibilities and authorities.
15. Information. Facts, data, or knowledge itself as opposed to the medium in which it is contained.
16. Local classification office. The organization within a field element that is responsible for handling classification/declassification-related issues.
17. Mandatory Review. A declassification review of a document containing RD/FRD information that is requested under 10 CFR Part 1045.42, or a document containing NSI that is requested under Section 3.6 of Executive Order 12958.
18. Material. Any substance regardless of its physical or chemical form, including any raw, in-process, or manufactured commodity, equipment, component, accessory, part, assembly, or product of any kind.
19. National Security Information (NSI). Information that has been determined pursuant to Executive Order 12958 and any predecessor orders to require protection against unauthorized disclosure and that is so designated. The levels Top Secret, Secret, and Confidential are used to designate such information.
20. Official Use Only.
  - a. A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act.
  - b. A security classification marking used from July 18, 1949, through October 22, 1951.
21. Original Classification. A determination by an Original Classifier that certain new information requires protection against unauthorized disclosure because of national security interests under Executive Order 12958; such information is identified as National Security Information.

22. Original Classifier. A Federal Government employee who is authorized to determine under Executive Order 12958 that certain new information requires protection against unauthorized disclosure in the interest of national security; such information is identified as National Security Information.
23. Permanent Records. Records appraised by the National Archives and Records Administration under Title 44 of the United States Code and determined to have sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes.
24. Portion Marking. The application of certain classification markings to individual words, phrases, sentences, paragraphs, or sections of a document to indicate their specific classification level and category (if RD or FRD).
25. Reclassification. A determination by an appropriate authority that restores the classification to (a) information that was classified as NSI and then declassified or (b) a document or material that was classified as RD, FRD, or NSI and then erroneously declassified.
26. Restricted Data (RD). All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.
27. Source Document. A classified document, other than classification guidance, from which information is extracted for inclusion in another document. Classification of the information extracted is determined by the classification markings shown in the source document.
28. Systematic Review. A periodic review of classified documents for declassification based on the degree of public and researcher interest and the likelihood of declassification upon review.
29. Upgrading. A determination by an appropriate authority that (a) assigns the correct classification level and/or category to a document or material that was erroneously issued as unclassified or (b) raises the classification level or category of a document or material to adequately protect the contents.
30. Variance. A method that differs from a directive requirement for a specific or indefinite period of time or for a specific project, but still meets that requirement by providing an equivalent level of implementation.
31. Waiver. Exemption from meeting a specific directive requirement.

# GUIDELINES ON EXPORT CONTROL AND NONPROLIFERATION



July 1999

U.S. Department of Energy  
Office of Nonproliferation and National Security  
Office of Arms Control and Nonproliferation  
Nuclear Transfer and Supplier Policy Division

**Guidelines on Export Control**  
**and**  
**Nonproliferation**

**Table of Contents**

<b>1.0</b>	<b>Purpose .....</b>	<b>3</b>
<b>2.0</b>	<b>Policy .....</b>	<b>5</b>
<b>3.0</b>	<b>Scope .....</b>	<b>8</b>
<b>4.0</b>	<b>Export Controls on Equipment, Materials, and Technology .....</b>	<b>11</b>
<b>5.0</b>	<b>Export Control of DOE Surplus .....</b>	<b>13</b>
	<b>5.1 Transfer of Surplus Property and “Deemed Exports”.....</b>	<b>13</b>
<b>6.0</b>	<b>Export Controlled Information .....</b>	<b>15</b>
	<b>6.1 How to Review for ECI .....</b>	<b>16</b>
	<b>6.2 How to Treat ECI .....</b>	<b>18</b>
	<b>6.3 ECI and OSTI .....</b>	<b>19</b>
	<b>6.4 ECI Responsibilities .....</b>	<b>20</b>
	<b>6.5 Recordkeeping on ECI .....</b>	<b>21</b>
	<b>6.6 Restrictions on Release of ECI .....</b>	<b>23</b>
	<b>6.7 Visits and Assignments, Foreign Travel, and “Deemed Exports” .....</b>	<b>22</b>
<b>7.0</b>	<b>Establishing Export Control Review .....</b>	<b>23</b>
<b>8.0</b>	<b>Developing Program or Facility Guidelines .....</b>	<b>24</b>
<b>Appendix 1</b>	<b>Useful Web Sites for Export Control .....</b>	<b>25</b>
<b>Appendix 2</b>	<b>Glossary of Acronyms .....</b>	<b>26</b>

## GUIDELINES ON EXPORT CONTROL AND NONPROLIFERATION

### 1.0

#### Purpose

These guidelines are intended to help Department of Energy (DOE) and DOE contractor personnel to implement a responsible, security-conscious, and consistent policy regarding DOE transfers of unclassified equipment, materials, and technology that could adversely affect U.S. security or commitments against the proliferation of weapons of mass destruction (WMD). Such transfers can take many forms; some examples are:

- Export of equipment, materials, or technology, including technical information, data, “know-how,” or services, that convey expertise.
- Cooperative Research and Development Agreements (CRADAs); work-for-others; patent assignments; equipment loans; donations or sales of surplus property or transfers to other federal, state, other public agencies, or the private sector.
- International and domestic exchange programs.
- Publications.
- Presentations at conferences or other forums.
- Visits or assignments of foreign nationals to DOE facilities.
- Foreign travel by DOE or DOE contractor employees.

- Other means of communication such as telephone calls, faxes, e-mail, mailings, or making DOE technology available on the Internet or any local net available to foreign nationals.

Even the methods of transfer that take place within the United States -- for example, the visit of a foreign national who gains access to DOE technology or the sale of DOE equipment that conveys technology -- may involve what the Departments of Commerce and State consider a "deemed export." In such cases, DOE and DOE contractors should ascertain the need for an export license before the access is granted or the equipment is sold.

When unclassified equipment, materials, or technology related to a nuclear, nuclear-related, or other WMD technology is transferred without restriction, among the beneficiaries may be nuclear proliferant or potential adversary countries. DOE maintains a list of countries considered sensitive for proliferation, national security, or terrorism reasons.

Of special concern are transfers related to nuclear weapons design and production, special nuclear material (SNM) production, and the sensitive technologies of the nuclear fuel cycle. Particular caution should be exercised when transferring items especially designed or prepared for use in nuclear fuel cycle activities or in the nuclear weapons program.

Uncontrolled transfer of weapons-related or sensitive technologies to countries of concern is contrary to U.S. commitments as a member of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Nuclear Suppliers Group (NSG) and the NPT Exporters Committee

(Zangger Committee), the Missile Technology Control Regime (MTCR), the Australia Group (AG) on chemical and biological weapons, and the Wassenaar Arrangement (WA) on control of dual-use and munitions goods and technologies. It would also run counter to U.S. nonproliferation policy and national security objectives as reflected in U.S. laws and regulations. DOE dismantlement of nuclear weapons, facilities, and related infrastructure makes the need for caution on transfers especially acute. Adherence to these guidelines will help to protect against the inadvertent transfer of sensitive unclassified equipment, materials, or information inimical to the interests of the United States.

## 2.0

### Policy

By international treaties and agreements, statutes, and policy, DOE is committed to encouraging scientific and technical exchanges that are mutually beneficial and are consistent with U.S. national security and nuclear nonproliferation objectives. As a member of the NPT, the United States is obligated, like all other nuclear-weapon state members, not to help other countries acquire nuclear weapons technology but, at the same time, to facilitate the transfer of technologies applicable to peaceful uses of nuclear energy to NPT adherents. Similar obligations regarding WMD flow from U.S. membership in the NSG and Zangger Committee, the MTCR, AG, and WA. DOE policy and procedures on the transfer of equipment and materials and the dissemination of scientific and technical information must balance the Department's commitment to U.S. nonproliferation and national security objectives against its commitments to sharing peaceful nuclear technology and to U.S. technological progress, scientific and energy objectives,

and support for U.S. industry. These sometimes conflicting commitments may require restricting such transfers, but only after careful consideration.

When it is necessary to control access to a technology, the primary means remains the classification system, augmented by the Unclassified Controlled Nuclear Information (UCNI) controls defined in Section 148 of the Atomic Energy Act. But legal, operational, scientific, or historical considerations make it impractical, ill-advised, or even impossible to classify *all* technology significant to national security or nonproliferation objectives. The transfer abroad of such unclassified but still sensitive technology is controlled by U.S. Government export laws and regulations.

For transfers of nuclear, nuclear-related, and other WMD-related equipment, materials and technology, U.S. Government export controls enforce the requirements of the Atomic Energy Act, the Nuclear Non-Proliferation Act, the Export Administration Act, and the Arms Export Control Act. These statutes and their implementing regulations require licenses from the Department of Commerce, Nuclear Regulatory Commission, or Department of State (DOS) or an authorization from the Secretary of Energy before certain unclassified nuclear, nuclear-related and other WMD commodities and technical information can be exported.

U.S. Government export control regulations reflect the export control lists of the NSG, an international organization of major nuclear supplier countries dedicated to nuclear nonproliferation. These NSG lists may be found in International Atomic Energy Agency Information Circular (INFCIRC) 254, as amended. The INFCIRC 254/Part 1 list comprises

equipment and materials especially designed or prepared for nuclear application and is known as the NSG Trigger List because the items on it "trigger" the imposition of International Atomic Energy Agency safeguards. The INFCIRC 254/Part 2 list comprises items which have both nuclear and non-nuclear applications and is known as the NSG Dual-Use List.

Pursuant to section 57 b. of the Atomic Energy Act, as implemented by DOE regulations 10 CFR Part 810, the Secretary of Energy's authorization is required for U.S. persons engaging directly or indirectly in the production of special nuclear material outside the United States. DOE also reviews license applications submitted to the Department of Commerce (DOC), the Department of State (DOS), and the Nuclear Regulatory Commission (NRC) for other nuclear and nuclear-related exports. DOE-sponsored activities often require the export of equipment, materials, or technology subject to DOC, DOS, or NRC license; in such cases, the DOE program office or contractor involved must obtain the required export license. But even when a DOE export falls within the scope of 10 CFR Part 810, DOE should conduct an export control review of the technology to be provided. A private sector export of such technology would be subject to authorization by the Secretary of Energy; lack of an export control review for DOE-sponsored exports could defeat the intent of the NPT, U.S. laws and regulations, and U.S. international commitments.

These guidelines describe requirements and methods for DOE export control review. They are intended to:

- Help identify equipment, materials, and technology requiring review and possible licensing or restriction.
- Encourage a reasoned weighing of proliferation and national security concerns against

program objectives, scientific and technological advance, or economic benefit when considering transfers of technology subject to export control.

### 3.0

#### Scope

These guidelines are applicable to all unclassified scientific and technical equipment, materials, and technology in the possession or control of DOE or its contractors which require an export license or authorization for transfer to another country. The U.S. Government export control regulations to be applied in accordance with these guidelines are:

- DOE's regulations 10 CFR Part 810, "Assistance to Foreign Atomic Energy Activities."
- Nuclear Regulatory Commission regulations 10 CFR Part 110, "Export and Import of Nuclear Materials and Facilities."
- Department of Commerce Export Administration Regulations (EAR) 15 CFR Part 730-774, especially 15 CFR Part 744, "Control Policy: End-User and End-Use Based," the discussion of Technical Data in 15 CFR 734, and 15 CFR 774 (Commerce Control List);
- Department of State regulations 22 CFR Parts 120-130, "International Traffic in Arms Regulations" (ITAR), especially Category 16.

The guidelines govern export control responsibilities not only at DOE sites but also for DOE-sponsored off-site activities, such as events at non-DOE locations or presentations or publications by DOE or DOE contractor personnel. However, they do not apply to requests for technical information submitted pursuant to the Freedom of Information Act; nor do they apply to

fundamental scientific and engineering research as defined in National Security Decision Directive (NSDD) 189.<sup>1</sup> Fundamental research, conducted to advance general knowledge, is normally not of export control concern. The results of such research are traditionally shared broadly throughout the international scientific community. However, in rapidly advancing research fields, fundamental research may develop practical applications that make it subject to export control. Further, fundamental research sometimes uses technologies or computational tools and techniques that may be sensitive and subject to export control. And in extraordinary circumstances fundamental research may be classified if it is particularly significant to national security. These guidelines do not affect procedures for dealing with the potential generation of classified information by fundamental research.

Another area in which export controls may not apply is U.S. Government negotiations with foreign governments or in international forums. When U.S. Government representatives engage in such discussions, under a License Exception granted by the Department of Commerce (Section 740.11 of the Export Administration Regulations), they may draw upon technical information that otherwise would require an export license for transmittal abroad. A good example would be transmittal of technical information deemed essential for U.S. engagement in arms control negotiations directed by the National Security Council. This License Exception applies, however, only when transmittal of the information results from an official interagency decision. An individual agency acting on its own may not convey export controlled technical information to

---

<sup>1</sup> NSDD 189 defines fundamental research as “basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.”

foreign government representatives without first obtaining an export license. But the same individual agency may convey export controlled technical information to foreign government representatives under the License Exception when empowered by a U.S. government decision that the agency shall do so.

Finally, according to the Department of Commerce Export Administration Regulations (15 CFR 779), in applying the Guidelines for export control purposes, DOE sites should treat foreign nationals who are lawfully admitted for permanent residence in the United States (Permanent Resident Aliens - PRA) as they do U.S. citizens; thus, transfer of technology to a PRA or giving a PRA access to DOE equipment or materials is not considered an export.

The areas of DOE export control concern embrace the full range of technologies pertinent to proliferation of weapons of mass destruction and to national security. For historical reasons, the main focus of DOE -- and these guidelines -- is on nuclear and nuclear-related technologies. These technology areas are described in the DOE Sensitive Subjects List and in much greater detail in DOE's Nuclear Technology Reference Book (NTRB), much of which is classified. But the range of technologies in which DOE is engaged goes far beyond the nuclear; it encompasses virtually all fields of weaponry, including missiles, conventional arms, and chemical and biological weapons, as well as many fields of peaceful research and development. Non-nuclear technologies are described in considerable detail in the Department of Defense's Militarily Critical Technologies List (MCTL). They also are included in the DOE Sensitive Subjects List. However, discussion of a technology in the NTRB, the MCTL, or the Sensitive Subjects List does not mean that *all* commodities associated with the technology require an export license. In this respect they differ

sharply from the export control lists of the NSG, the MTCR, the AG, and the WA; all equipment, materials and technology described in these lists are export controlled by the member countries. Therefore, U.S. export control regulations cover all items on these lists.

#### 4.0 Export Controls on Equipment, Materials, and Technology

Qualified DOE or DOE contractor personnel considering the transfer of equipment, materials, or technologies must conduct an export control review prior to any such transfer. The transfer may not be an export, but the review is required for both foreign and domestic transfers (e.g., public auction, donation, direct sale, cooperative program, work-for-others, transfers to other agencies, off-site events, information exchange, public presentation, publication, foreign travel, shipment, mail, fax, e-mail, or webpage).

If the transfer involves an export by DOE or a DOE contractor to another country -- for example, a loan or other transfer of equipment as part of a program of cooperation -- DOE or a DOE contractor must obtain any necessary export license. But bear in mind that some exports can take place entirely within the United States. DOC and DOS consider domestic release of technology to a foreign national who is not a U.S. permanent resident a "deemed export" to that person's country. Therefore, a DOE laboratory may need to obtain an export license before letting a foreign national who is not a PRA purchase or otherwise have access to its equipment, materials, or technology. For example, an export license may be required for a non-PRA foreign national to buy at auction a surplus DOE computer whose export to the foreign national's country would require an export license or for the foreign national to have access to the computer during an

assignment at a DOE laboratory.

However, even if a transfer is to U.S. citizens entirely within the United States, DOE policy requires that an export control review be made. For example, a transfer of DOE equipment, materials, or technology via public auction or CRADA agreement, must include export control guidance in the sale contract or other transfer agreement; and the agreement must require that DOE's export control guidance be passed on in the event of retransfer, including any domestic retransfer. In some agreements, DOE approval should be required for retransfer. Whatever conditions are imposed on a transfer, the responsible DOE site must maintain records showing the conditions . . .

U.S. export controls on nuclear, nuclear-related, dual-use and military-related commodities are published in DOE's regulations 10 CFR Part 810; Nuclear Regulatory Commission regulations 10 CFR Part 110; Department of Commerce Export Administration Regulations (EAR) 15 CFR Part 730-774, especially 15 CFR Parts 734, 744, and 774 (Commerce Control List); and Department of State regulations 22 CFR Parts 120-130, especially Category 16.

DOE and DOE contractor personnel familiar with these export control regulations can generally determine the requirements for a given item without further assistance. Personnel not familiar with the regulations should first consult the NSG control lists cited earlier; if an item is on an NSG list, it is covered in U.S. Government export control regulations. In regard to nonnuclear items, personnel not familiar with export control regulations or seeking greater technical detail should consult the Sensitive Subjects List, the MCTL or, if need be, the lists of the relevant

multinational export control regime. Most important, DOE's Nuclear Transfer and Supplier Policy Division (NN-43) and almost all DOE sites have personnel who regularly deal in export control matters and can provide assistance as necessary.

## **5.0 Export Control of DOE Surplus**

DOE property transfers, of surplus property or otherwise, must take place in accordance with DOE Property Management Regulations 41 CFR 109. DOE property being transferred in surplus or other sales, loans, donations, CRADAs, work-for-others agreements, cooperative agreements, inter-agency transfers, or technical exchange programs that is determined to be subject to export control should be designated as such. The recipients should be informed in writing of their responsibility to obtain required export licenses or authorizations for retransfer to another country. Recipients also should be required to pass on DOE's export control guidance if they retransfer the property domestically.

### **5.1 Transfer of Surplus Property and "Deemed Exports"**

In some cases an export license may be needed for even a domestic transfer of surplus property to a foreign national. For example, the sale of DOE surplus equipment to a foreign national in the United States may constitute a "deemed export" because the foreign national thereby gains access to the technology inherent in the equipment. Therefore, before transferring title to export controlled DOE property to a foreign national, DOE or DOE contractor officials should ascertain whether a "deemed export" may occur. If so, and if a DOC or DOS license would be needed to

export the item to the foreign national's country, DOE must obtain the license before the property changes hands. DOC or DOS export control authorities must be consulted and the discussion documented in such cases

Export control review of surplus property may determine that it should be rendered useless for nuclear purposes before being offered to the public or that the sales agreement should require its disposal as scrap. In some cases, the review may determine that the property is too sensitive for sale or other transfer and, therefore, that it must be destroyed by DOE. Surplus equipment or materials especially designed or prepared for nuclear use will be either sold for scrap after being made useless for nuclear purposes or will be destroyed; the same will be done for weapons components. To establish whether equipment or materials are especially designed or prepared for nuclear use, consult Part 1 of the NSG lists (INFCIRC 254). All items on the Part 1 list are especially designed or prepared and, therefore, carry a "presumption of destruction." The same presumption applies to nuclear weapon components. But the presumption of destruction may be appealed and alternative disposition approved on a case-by-case basis. Such appeals must be made to the Assistant Secretary for Nonproliferation and National Security (NN-1). If the appeal is granted and alternative disposition is approved for NSG Trigger List items or weapons components, precautions must be taken to prevent any use inconsistent with U. S. Government nonproliferation or national security policy. This may require physically modifying equipment prior to transfer, placing conditions in the transfer agreement, or both.

Export Controlled Information (ECI) is a category of information DOE established more than a decade ago as a nonproliferation tool. ECI is defined as unclassified technical information whose export is subject to export control and whose unrestricted public dissemination could help proliferants or potential adversaries of the United States.

To understand why DOE established the ECI category, consider how a private firm treats its technology. The profit motive restrains the firm from making its technical information, technical data, technical expertise, and “know-how” publicly available. The profit motive does not restrain U.S. Government agencies, which are encouraged to freely disseminate information to the public, with appropriate safeguards. But public dissemination of technology is, in effect, to export it to all countries, and some DOE technology -- even unclassified technology -- could help proliferants or potential adversaries. Therefore, DOE requires an ECI review before public release of technology that could help proliferants or potential adversaries; and just as a U.S. Government agency may deny an export license for technology posing proliferation concerns, DOE may restrict dissemination of ECI. An ECI review must be conducted before publication of DOE technology that could help proliferants or potential adversaries or its presentation at a conference open to foreign nationals. Further, export licensing requirements must be met for any export of ECI, including “deemed export” transfer to foreign nationals at DOE sites; and anyone given access to ECI at a DOE site must comply with export licensing requirements before retransfer of the ECI to foreign nationals. Site managers are responsible for ensuring that required ECI reviews are performed.

## 6.1

### How to Review for ECI

The fact that technical information deals with items discussed in the NSG lists, the NTRB or MCTL is not by itself sufficient reason to withhold it from public release; rather, it is a reason to review the specific technical information involved to determine whether limiting release is warranted.

By checking the NSG lists or U.S. export control regulations, the reviewer can establish whether the technology, if proposed for export, would require a U.S. Government export license or authorization. If so, the reviewer can determine whether it should be released publicly by posing a series of questions:

- Could uncontrolled release reasonably be expected to contribute to nuclear proliferation? Could it help a proliferant significantly to improve its ability to develop nuclear weapons or gain know-how for producing or preparing nuclear weapons materials?
- Could uncontrolled release reasonably be expected to adversely affect U.S. national security? Could an adversary country gain significant technical advantage, negate a U.S. advantage, or find it significantly easier to develop advanced weapons or make other military progress?
- Is the technical information of such character that association with its source -- for example, a DOE weapons laboratory -- would implicitly enhance its value to a proliferant or adversary?

If the reviewer concludes that unlimited dissemination would adversely affect U.S. nonproliferation objectives or national security, the technical information should be designated

ECI, with appropriate markings, and its *uncontrolled* dissemination, especially uncontrolled *foreign* dissemination, should be prevented. However, designation as ECI does not prevent sharing of the information among DOE or DOE contractor employees. With appropriate precautions and obtaining an export license when required, ECI also can be transferred under work-for-others agreements, exchanges based upon agreements for international cooperation, exchanges under U.S.-approved programs of the International Atomic Energy Agency, or exchanges with countries posing no proliferation or national security concerns. As noted earlier, DOE maintains a list of countries considered sensitive for reasons of national security, nonproliferation, foreign policy, or support of terrorism.

Markings to be affixed to technical information determined to be ECI may vary depending on the needs and preferences of site or program managers.

The following format is preferred:

#### *EXPORT CONTROLLED INFORMATION*

*Contains technical information whose export is restricted by statute. Violations may result in administrative, civil, or criminal penalties. Limit dissemination to U.S. Department of Energy employees and contractors and other U.S. Government agencies. The cognizant program manager must approve other dissemination. This notice shall not be separated from the attached document.*

*Reviewer (Signature)*

*Date*

Sites that have developed their own ECI marking formats may retain them as long as they contain at least the information elements of the preferred format.

DOE scientists and engineers, technology security experts, export control specialists, facility shipping offices, classification officers, property management personnel, and legal departments all may have roles to play in the export control review process. Technical input by individuals familiar with the equipment, materials, or technology involved may be essential to identifying potentially sensitive commodities or technologies or to determining applicable export controls. Such technical experts may also know best how, for example, to render proliferation-sensitive equipment useless to a nuclear proliferant but still useful for nonnuclear purposes or as scrap. At some sites, the certification that an ECI review has been made may best be accomplished simultaneously with declassification review. Classification offices should have copies of the NTRB, the MCTL, and the pertinent export control regulations.

If technology is determined to be ECI, it should be released domestically only to a controlled distribution, such as a U.S. firm that is party to a CRADA or a technical exchange agreement, or a U.S. purchaser of surplus property. Bear in mind that a U.S. firm dealing with DOE in a CRADA, work-for-others arrangement or other contractual agreement may be foreign-owned; in such cases, the U.S. firm may need to obtain an export license before transferring DOE technical information, equipment, or material to its foreign parent.

ECI should be protected as far as legally allowable from release to foreign countries, organizations, or individuals unless authorized by the appropriate Headquarters program manager. Such protection should be especially afforded -- again, as far as legally allowable -- to ECI sought

by nationals of countries on DOE's Sensitive Country List. ECI documents should *not* be made available on the Internet or a local net available to foreign nationals. If technical information is controlled by DOE under its Part 810 regulations, then a DOE program manager may direct its release to foreign recipients as part of a DOE program. If the program manager is acting pursuant to a technical cooperation agreement; the agreement itself should have been approved by the Assistant Secretary for Nonproliferation and National Security. If the agreement was not approved and the information is ECI, the Nuclear Transfer and Supplier Policy Division should be consulted before the ECI is transferred.

For foreign nationals at DOE facilities to be given access to ECI, a DOC or DOS license, granting approval of the "deemed export," must be obtained; likewise DOE or DOE contractor employees traveling abroad should not disseminate ECI without an Individual Validated License granted by the appropriate licensing authority. However, under current law, a report sought under the Freedom of Information Act may not be withheld on grounds that the report contains ECI.

### 6.3

### ECI and OSTI

ECI review should be initiated early enough to avoid conflicts with planned publication, presentation, distribution, or visit schedules, and should be consistent with guidelines implementing DOE Order 241.1 of August 17, 1998, that require contractors or Operations or Program Offices to forward reports to the Office of Scientific and Technical Information (OSTI), Oak Ridge, Tennessee, with a completed DOE Form 241.1, Announcement of Department of

Energy (DOE) Scientific and Technical Information (STI). The form sent to OSTI records the outcome of the ECI review, including dissemination guidance. When no dissemination guidance is given, OSTI will provide the report on request only to DOE and its major U.S. contractors or to other U.S. Government agencies unless the responsible program manager advises otherwise.

#### 6.4

#### ECI Responsibilities

The author of a technical document should be consulted in the ECI review of the document. DOE and DOE contractor personnel reviewing their own documents for ECI should inform their supervisors of their findings. Supervisors should ascertain that the reviewers are technically qualified and have an understanding of the factors involved in technology transfer. Supervisors also should document that ECI issues have been considered as part of the clearance process for a publication, meeting presentation, response to a foreign request for technical information, or security plan for controlling access by a foreign national. The overall ECI review process at each site should be approved by the site manager.

A reviewer who determines that information constitutes ECI will indicate the permissible domestic dissemination. For example, a reviewer may authorize dissemination only to DOE and its major contractors or to all Federal agencies and their U.S. contractors. The reviewer may attach to the document a list of authorized recipients or a "non-dissemination" list of sensitive countries. In any case, ECI dissemination guidance is intended to prevent the domestic release of technology by OSTI or any other DOE entity to unauthorized foreign governments, firms, and individuals unless it is reviewed and approved for release by the Headquarters Program Office. A

Headquarters Program Office authorizing release to an otherwise unauthorized recipient must notify the reviewing office and OSTI of the action. A Headquarters Program Office intending to export ECI must take care that any required export license is obtained.

#### **6.5 Recordkeeping on ECI**

ECI documentation will be maintained at reviewing offices and be available to Headquarters program managers and to the Nuclear Transfer and Supplier Policy Division, NN-43. The documentation should include foreign requests for material determined to be ECI, the disposition of the request, and the reason therefor. Headquarters program managers should monitor review activities periodically to assure uniformity and consistency with DOE policy as reflected in these guidelines.

#### **6.6 Restrictions on Release of ECI**

An ECI review finding that a proposed release is inconsistent with nonproliferation or national security policy may require revision of either the content or dissemination of the technical information. Just as DOE sometimes denies a firm's request for authorization to export technology or sets conditions on the authorization, DOE may, in the case of publication of ECI or its presentation at an international meeting, determine that U.S. policy requires that some technical content be excised or that participation by nationals of sensitive countries in the meeting be restricted. In the latter case, meeting participants must sign a commitment not to transmit the ECI to sensitive country nationals and to advise other recipients of the ECI restrictions. Abstracts

or proceedings associated with such verbal presentations also must be reviewed.

**6.7 Visits and Assignments, Foreign Travel, and “Deemed Exports”**

In the case of a visit or assignment of a foreign national to a DOE facility, measures should be taken to control access to export controlled equipment, materials or technology, and necessary export licenses must be obtained. Bear in mind that acquisition of DOE technology by the foreign national may be a “deemed export” requiring an export license before the foreign national is given access. Similarly, a DOE or DOE contractor employee going abroad should consider whether technology to be conveyed in planned discussions requires an export license; if so, an export license should be obtained before the trip.

Hosts of foreign visitors or assignees should familiarize themselves with the requirements of pertinent DOE Orders and the DOE-wide computerized Foreign Access Records Management System (FARMS). In planning visits and assignments, hosts should consult DOE’s Sensitive Country List and the Sensitive Subjects List, as well as lists of sensitive subjects developed at some of the national laboratories; these latter are narrower in scope than the Department-wide list but may offer more specificity on the subjects that are likely to be encountered at a particular site. In an era of increasing collaboration between U.S. and foreign scientists, engineers, and other technical personnel at DOE facilities, transfers of technology during such collaboration must adhere to U.S. export control laws and regulations. Export control requirements must be considered in determining the appropriateness of foreign national access to DOE technology. Foreign nationals from sensitive countries may need a license to acquire many technologies and all

foreign nationals may need a license to acquire certain technologies.<sup>2</sup>

Similarly, DOE travelers should familiarize themselves with the pertinent DOE Orders and the requirements of the computerized Foreign Travel Management System.

## 7.0 Establishing Export Control Review

Most DOE facilities, laboratories, and other sites already have developed structures to deal with export control review, technology security, ECI, declassification, and related issues. Requiring a rigid one-size-fits-all scheme is not practical, but site management is responsible for modifying site organization as necessary to ensure that the increased export control review responsibilities called for by these Guidelines are fulfilled, as well as the needs of each site. DOE believes this approach will lead to the most effective export control review program at each site.

When no export control review mechanisms exist, it is the responsibility of Headquarters offices, field offices, program managers, and contractor organizations to establish them as necessary. If differences emerge regarding facility guidelines or their application, or if review bodies in contractor organizations or field offices are unable to make a clear determination regarding a planned publication, presentation, sale of surplus property, donation, CRADA or other transfer, they should refer the matter to the responsible Headquarters program office. If necessary, the Headquarters program office should seek the advice of the Nuclear Transfer and Supplier Policy

---

<sup>2</sup> This guidance is not intended to preclude access by DOE or contractor employees who are foreign nationals from sensitive countries if they are permanent resident aliens under the Immigration and Naturalization Act.

Division, Office of Arms Control and Nonproliferation, Telephone (202) 586-2331, Fax (202) 586-1348.

8.0

Developing Program or Facility Guidelines

As experience is gained, program managers, laboratories, and other contractor facilities may decide they need more detailed "program guidelines" or "facility guidelines" for their specialized areas of activity. Such guidelines may be prepared by program managers and other experts familiar with the technologies involved. However, to ensure consistency among locally prepared and applied guidelines, these should be reviewed by the appropriate Headquarters Program Office in coordination with the Nuclear Transfer and Supplier Policy Division.

## APPENDIX 1

### Useful Web Sites for Export Control

- Department of Commerce Export Administration Regulations -  
<http://www.access.gpo.gov/nara/cfr/cfr-table.serch.html>
- Department of Energy Regulations 10 CFR Part 810 -  
[http://www.access.gpo.gov/nara/cfr/waisidx/10cfr810\\_99.html](http://www.access.gpo.gov/nara/cfr/waisidx/10cfr810_99.html)
- Department of State International Traffic in Arms Regulations – 22 CFR 120-130 -  
<http://www.pmdtc.org/itar2.htm>
- Militarily Critical Technologies List -  
<http://www.dtic.mil/mctl>
- Missile Technology Control Regime Guidelines -  
<http://www.acda.gov/export.htm>
- Nuclear Regulatory Commission 10 CFR 110 -  
<http://www.nrc.gov/NRC/CFR/index.html>
- Nuclear Suppliers Group Guidelines – INFCIRC 254 Parts I and II -  
<http://www.iaea.org/worldatom/infcircs/inf201-300.html>
- Nonproliferation Treaty Exporters Committee (Zangger) INFCIRC 209 -  
<http://www.iaea.org/worldatom/infcircs/inf201-300.html>
- Wassenaar Arrangement Control Lists -  
<http://www.wassenaar.org>

## APPENDIX 2

### Glossary of Acronyms

AG	-	Australia Group
CRADA	-	Cooperative Research and Development Agreement
CRD	-	Confidential Restricted Data
DE	-	Directed Energy
EAR	-	Department of Commerce's Export Administration Regulations
ECI	-	Export Controlled Information
ICF	-	Inertial Confinement Fusion
INFCIRC	-	Information Circular of the International Atomic Energy Agency
ITAR	-	Department of State's International Traffic in Arms Regulations
MCTL	-	Department of Defense's Militarily Critical Technologies List
MTCR	-	Missile Technology Control Regime
NPT	-	Treaty on the Non-Proliferation of Nuclear Weapons
NSG	-	Nuclear Suppliers Group
NTRB	-	Nuclear Technology Reference Book
OSTI	-	Office of Scientific and Technical Information
PRA	-	Permanent Resident Alien
R&D	-	Research and Development
SNM	-	Special Nuclear Material
SRD	-	Secret Restricted Data
UCNI	-	Unclassified Controlled Nuclear Information
WA	-	Wassenaar Arrangement
WMD	-	Weapons of Mass Destruction