ORDER

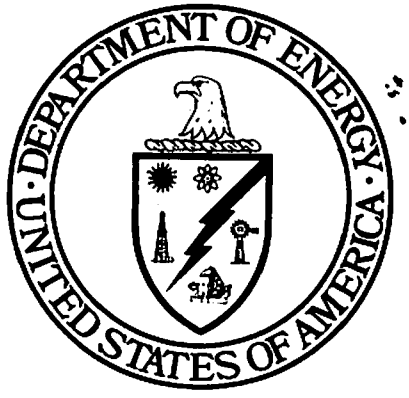
DOE 5650.2A

5-8-85

Cancelled by DOE 5650.2B 12-31-91

DEPARTMENT OF ENERGY

CLASSIFICATION OF INFORMATION MANUAL



U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5650.2A

5-8-85

SUBJECT: CLASSIFICATION OF INFORMATION

Cancelled by DOE 5650.2B 12-31-91

1. PURPOSE. To specify responsibilities, authorities, policy, and procedures for the management of the Department of Energy (DOE) classification system.

2. CANCELLATION. DOE 5650.2, CLASSIFICATION OF INFORMATION, of 12-12-78.

3. SCOPE. The provisions of this Order apply to all Departmental Elements and contractors and subcontractors performing work for the Department as provided by law and/or contract and as implemented by the appropriate contracting officer.

4. REFERENCES.

   a. Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011-2296 (Atomic Energy Act), which established procedures for control of atomic energy information.

   b. Department of Energy Organization Act of 1977, Public Law 95-91, which created DOE.

   c. DOE Delegation Order No. 0204-2, 10-1-77, which authorizes the Assistant Secretary for Defense Programs (DP-1) to direct and administer the DOE classification program, based on the Atomic Energy Act.

   d. DOE Delegation Order No. 0204-101, of 8-1-82, which authorizes DP-1 to direct and administer the DOE information security program, based on Executive Order 12356.

   e. Energy Reorganization Act of 1974, as amended, Public Law 93-438, which created the Energy Research and Development Administration (ERDA) and the Nuclear Regulatory Commission (NRC).

   f. Executive Order 10290, "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information which Requires Safeguarding in the Interest of the Security of the United States," of 9-24-51 (superseded by Executive Order 10501).

   g. Executive Order 10501, as amended, "Safeguarding Official Information in the Interests of the Defense of the United States," of 11-5-53 (superseded by Executive Order 11652), which established requirements concerning classification of defense information.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Classification

h. Executive Order 10964, "Amendment of Executive Order No. 10501 Entitled 'Safeguarding Official Information in the Interests of the Defense of the United States,'" of 9-20-61 (superseded by Executive Order 11652), which amended classification requirements of Executive Order 10501.

i. Executive Order 11652, as amended, "Classification and Declassification of National Security Information and Materials," of 3-8-72 (superseded by Executive Order 12065), which provided new requirements concerning classification of information.

j. Executive Order 12065, "National Security Information," of 6-28-78 (superseded by Executive Order 12356), which provided new requirements concerning classification of information.

k. Executive Order 12356, "National Security Information," of 4-2-82, 3 CFR 166 (1983), which provides new requirements concerning classification of information.

l. Freedom of Information Act of 1967, as amended (hereinafter referred to as the Freedom of Information Act (FOIA)), which established requirements for public access to Government information.

m. Information Security Oversight Office Directive No. 1, "National Security Information," of 6-23-82, 32 CFR 2001 (1984), which supplements Executive Order 12356.

n. National Security Act of 1947, as amended, Public Law 80-253, which created the Department of Defense (DOD).

o. Patent Secrecy Act of 1952, Public Law 82-593, which established authority for imposing secrecy on patents of importance to the national security.

p. Presidential Order, "National Security Information," of 5-7-82, 3 CFR 257 (1983), in which the President authorizes particular officials to classify information originally (the Secretary of Energy is granted Top Secret Original Classification Authority).

q. Privacy Act of 1974, 5 U.S.C. 552a, which established requirements for Government protection of personal information.

BY ORDER OF THE SECRETARY OF ENERGY:

WILLIAM S. HEFFELFINGER
Director of Administration

TABLE OF CONTENTS

CHAPTER II - RESPONSIBILITIES AND AUTHORITIES

CHAPTER III - POLICY AND OBJECTIVES

CHAPTER IV - CLASSIFICATION CRITERIA AND LEVELS

CHAPTER V - CLASSIFICATION OF INFORMATION AND DOCUMENTS

CHAPTER VII - EDUCATION

CHAPTER VIII - CLASSIFICATION APPRAISALS

CHAPTER IX - CLASSIFICATION VIOLATIONS

CHAPTER X - REFERENCES AND OPERATING PROCEDURES

CHAPTER I

ABBREVIATIONS AND DEFINITIONS

1. ABBREVIATIONS.

   a. C - Confidential.

   b. D6 - Downgrade in 6 years.

   c. D8 - Downgrade in 8 years.

   d. D10 - Downgrade in 10 years.

   e. DOD - Department of Defense.

   f. DOE - Department of Energy.

   g. DP-1 - Assistant Secretary for Defense Programs.

   h. DP-32 - Director of Classification.

   i. DP-34 - Director of Safeguards and Security.

   j. EO - Executive Order.

   k. ERDA - Energy Research and Development Administration.

   l. FERC - Federal Energy Regulatory Commission.

   m. FOIA - Freedom of Information Act.

   n. FRD - Formerly Restricted Data.

   o. FRUS - Foreign Relations of the United States.

   p. GC-42 - Assistant General Counsel for Patents.

   q. GDS - General Declassification Schedule.

   r. HQ - Headquarters.

   s. ISOO - Information Security Oversight Office.

   t. NRC - Nuclear Regulatory Commission.

   u. NSI - National Security Information.

   v. OADR - Originating Agency's Determination Required.

   w. OUO - Official Use Only.

x. RD - Restricted Data.

y. R&D - Research and Development.

z. REV20 - Review in 20 years.

aa. REV30 - Review in 30 years.

bb. S - Secret.

cc. SCI - Sensitive Compartmented Information.

dd. TS - Top Secret.

ee. UCNI - Unclassified Controlled Nuclear Information.

ff. XGDS - Exempt from the General Declassification Schedule.

2. DEFINITIONS. For the purpose(s) of this Order, these definitions also include other Federal agencies and their contractors and subcontractors performing work for DOE under Interagency Agreements and financial assistance recipients whose efforts involve classified information.

a. Administrative Information is that required or generated in the normal functioning of an organization or program, other than technical, costing, or programmatic information.

b. Authorized Classifier.

(1) Original Classifier. One authorized to classify National Security Information (NSI) by an original determination based on Executive Order 12356, where no specific guidance exists.

(2) Derivative Classifier. One authorized to classify documents or material as Restricted Data (RD), Formerly Restricted Data (FRD), or NSI only in accordance with existing guidance.

c. Authorizing Official. See "Denying Official," paragraph 2bb, below.

d. Classification.

(1) Original Classification. The initial determination that information requires protection as NSI under the provisions of Executive Order 12356. Includes the specification of a classification level and the classification duration.

(2) Derivative Classification.

(a) Restricted Data or Formerly Restricted Data. A determination in accordance with approved classification guidance or source documents that a document or material contains RD or FRD.

(b) National Security Information. A determination in accordance with approved classification guidance, source documents, or other instructions from an Original Classifier that a document or material contains NSI.

e. Classification Appraisal. A systematic process by which a judgment is made of the quality of a classification program.

f. Classification Authority.

(1) Original Classification Authority. Authority to originally classify documents or material as NSI.

(2) Derivative Classification Authority. Authority to derivatively classify documents or material as RD, FRD, or NSI.

g. Classification Boards are appointed by Heads of Field Elements or prime contractor organizations or Classification Officers to assist them in discharging their classification and declassification responsibilities.

h. Classification Category. One of the three kinds of classified information: Restricted Data, Formerly Restricted Data, or National Security Information.

i. Classification Guide. A document containing classification guidance for the use of Authorized Classifiers and Derivative Declassifiers in making classification determinations.

j. Classification Level. One of the three classification specifications: Top Secret, Secret, Confidential.

k. Classification/Security Markings are affixed to classified documents or material to indicate, among other things, the classification category of information contained therein (i.e., RD, FRD, or NSI), the classification level (i.e., Top Secret, Secret, or Confidential) or the designation "Unclassified," and the date or event for declassification for NSI.

l. Classification Officer.

(1) Department of Energy Classification Officer. One designated by the Head of a Field Element to administer its classification program and oversee or monitor the classification programs of contractor organizations under its jurisdiction.

(2) Contractor Classification Officer. One designated by the head of a contractor organization to administer its classification program and oversee or monitor the classification programs of subcontractor organizations under its jurisdiction.

m. Classification Policy. DOE policy on classification, transclassification, downgrading, and declassification of information under its purview.

n. Classification Violation. Willful abuse of the classification provisions of the Atomic Energy Act, Executive Order 12356 and its implementing directives, other statutes or executive orders pertaining to classification, this Order, or approved classification guidance.

o. Classified Document. Any document containing classified information.

p. Classified Information requires protection against unauthorized disclosure in the interest of national security and includes RD, FRD, and NSI.

q. Confidential. The lowest classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

r. Confidential Source. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or identity of the source, or both, will be held in confidence.

s. Contractor Classification Officer. See "Classification Officer," paragraph 21, above.

t. Contractor Organization. For the purpose(s) of this Order, the definitions in subparagraphs t(1) and (2) also include other Federal agencies and their contractors and subcontractors performing work for DOE under Interagency Agreements and financial assistance recipients whose efforts involve classified information.

(1) Prime Contractor Organization. An organization under direct contract at any tier to DOE.

(2) Subcontractor Organization. An organization under contract at any tier to a DOE contractor organization.

u. Declassification.

(1) A determination by appropriate authority that information is no longer classified; or

(2) A determination by appropriate authority in accordance with approved classification policy or guidance that a classified document or material no longer contains classified information; or

(3) The removal or cancellation of classification markings from a document or material in accordance with a declassification notice from an appropriate authority.

v. Declassification Authority. Authority to determine that information, documents, or material can be declassified and to effect such declassification.

w. Declassification Event. An event that would eliminate the need for continued classification.

x. Declassification Guidance. Guidance provided by appropriate authority for use in declassifying documents or material. It may be used only by those with declassification authority.

y. Declassification Policy. DOE policy on declassification of information.

z. Declassified Document. A previously classified document that has been declassified in accordance with approved declassification policy and from which the classification markings have been removed or cancelled.

aa. Declassified Information. Previously classified information that has been declassified by appropriate authority.

bb. Denying Official. A DOE official authorized to make initial determinations for DOE to deny, in whole or in part, requests for records under the FOIA. (With respect to determinations to release information, referred to as an "Authorizing Official.")

cc. Departmental Element. A Headquarters (HQ) Element or a field element.

(1) Headquarters Element. For purposes of this Order, an organization at or above the office level (level 3) located within the Washington, DC, metropolitan area, or in the case of the Office of Scientific and Technical Information, located in Oak Ridge, Tennessee.

(2) Field Element. For purposes of this Order, an operations office, power administration, regional office, or Naval Reactors field office.

dd. Department of Energy Classification Officer. See "Classification Officer", paragraph 21, above.

ee. Derivative Classification. See "Classification," paragraph 2d, above.

ff. Derivative Classification Authority. See Classification Authority," paragraph 2f, above.

gg. Derivative Classifier. See "Authorized Classifier," paragraph 2b, above.

hh. Derivative Declassifier. One authorized to downgrade and declassify documents or material.

ii. Document. Any record of information regardless of physical form or characteristics, including, but not limited to, the following:

(1) All handwritten, printed, or typed matter;

(2) All painted, drawn, or engraved matter;

(3) All sound, magnetic, electromechanical, or optical recordings;

(4) All photographic prints, exposed or developed film, and still or motion pictures;

(5) Automatic data processing input, memory, program, or output information or records such as punch cards, tapes, memory drums or disks, or visual displays; and

(6) All reproductions of the foregoing by any process.

jj. Downgrading. Lowering the classification level of information, documents, or material (does not include declassification).

kk. Field Element. See "Departmental Element," paragraph 2cc, above.

ll. Foreign Government Information.

(1) Information provided by a foreign government or an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government(s) or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

mm. Formal Report. A formal topical or progress report distributed in accordance with specific categories of the Standard Distribution Lists DOE/TIC-4500 for unclassified information and M-3679 for classified information, and by other lists as designated by the Manager of Scientific and Technical Information.

nn. Formerly Restricted Data. Classified information jointly determined by DP-1 and the DOD to be related primarily to the military utilization of

atomic weapons, and removed by DP-1 from the RD category pursuant to section 142(d) of the Atomic Energy Act.

oo. Government Agency. Any executive department, commission, independent establishment, or corporation, wholly or partly owned by the United States of America, which is an instrumentality of the United States, or any board, bureau, division, service, office, officer, authority, administration, or other establishment in the Executive Branch of the Government.

pp. Headquarters Classification Representative. An individual appointed by his or her element to serve as the point of contact with DP-32 on classification policies and procedures and to assist others in their classification and declassification responsibilities and authorities.

qq. Headquarters Element. See "Departmental Element," paragraph 2cc, above.

rr. Information. In this Order, information means facts, data, or knowledge itself, rather than the medium of its conveyance. (Documents and materials are deemed to convey or contain information and are not considered to be information per se.)

ss. Information Security Oversight Office. An organization within the General Services Administration responsible for overseeing Government implementation of Executive Order 12356.

tt. Local Classification Guide. A classification guide prepared and issued by DOE or a DOE contractor organization for a specific facility or activity. It is based on one or more program classification guides and provides detailed classification guidance.

uu. Mandatory Review. A declassification review that can be initiated or requested by a member of the public, a Government employee, or another Government agency pursuant to Executive Order 12356 and this Order.

vv. Material. Any substance regardless of its physical or chemical form (e.g., chemicals, raw materials, fabricated or processed items, machinery, or equipment).

ww. National Security. The national defense and foreign relations of the United States.

xx. National Security Information. Information pertaining to national security and classified in accordance with an Executive Order.

yy. Office of Classification. In this manual, the Office of Classification, DOE-Headquarters.

zz. Office of Safeguards and Security. In this manual, the Office of Safeguards and Security, DOE-Headquarters.

aaa. Official Information. Any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or under the control of the United States Government.

bbb. Official Use Only.

(1) A designation identifying unclassified information that may be exempt from mandatory disclosure under the FOIA; or

(2) A former (7-18-49 through 10-22-51) security classification marking.

ccc. Original Classification. See "Classification," paragraph 2d, above.

ddd. Original Classification Authority. See "Classification Authority," paragraph 2f, above.

eee. Original Classifier. See "Authorized Classifier," paragraph 2b, above.

fff. Portion Marking. The application of NSI classification markings to individual portions of a document to indicate their specific classification.

ggg. Prime Contractor Organization. See "Contractor Organization," paragraph 2t, above.

hhh. Program Classification Guide. A guide that states specific classification policy for a particular DOE program and provides the basis for the development of local guides.

iii. Reclassification. Restoration of classification to information previously classified as NSI and then declassified.

jjj. Responsible Reviewers. Those appointed to advise the Director of Classification (DP-32) on classification and declassification of matters in their fields of professional competence.

kkk. Restricted.

(1) A former U.S. security classification marking (prior to 12-15-53); or

(2) An active security classification marking used by some foreign governments and international organizations.

lll. Restricted Data. All data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act:

(1) Design, manufacture, or utilization of atomic weapons;

(2) Production of special nuclear material; or

(3) Use of special nuclear material in the production of energy.

mmm. Sanitizing. In this manual, the physical removal of all classified information from a classified document.

nnn. Secret. The classification level between Confidential and Top Secret, applied to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

ooo. Sensitive Compartmented Information. All information and material requiring special control for restricted handling under compartmented foreign intelligence systems.

ppp. Source Document. A document, other than a classification guide, from which information is extracted for inclusion in another document. The term "source document" is used in the context that the classification of information extracted from the source document is determined by reference to the classification specified in the source document for the information extracted.

qqq. Subcontractor Organization. See "Contractor Organization," paragraph 2t, above.

rrr. Systematic Review. The classification review under Executive Order 12356 in which the Archivist of the United States, acting under the Federal Records Act, determines which NSI records and Presidential papers or records are of sufficient historical value or other value to warrant permanent retention.

sss. Systematic Review Guidelines. Guidelines required by Executive Order 12356 for identifying NSI or documents containing NSI that may not be declassified automatically by the National Archives at 30 years.

ttt. System Manager. The DOE official responsible for a DOE system of records as designated in the system notice of that system published by DOE in the "Federal Register" in accordance with the provisions of the Privacy Act of 1974.

uuu. Top Secret. The highest classification level, applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

vvv. Transclassification. The removal of information from the RD category and its placement in the FRD category in accordance with section 142(d) of the Atomic Energy Act or the NSI category in accordance with section 142(e). (Does not include declassification.)

www. Unclassified. The designation for information, a document, or material that has not been classified or that has been declassified by proper authority.

xxx. Unclassified Controlled Nuclear Information. Certain unclassified Government information prohibited from unauthorized dissemination under section 148 of the Atomic Energy Act.

yyy. Upgrading. Raising the classification level of information, documents, or material, including correction of classification on such items erroneously issued as unclassified or at too low a classification level.

zzz. Visual Materials. Photographs, motion pictures, slides, artists' concepts, engineering drawings, plant layouts, plots, plans, maps, and so forth.

CHAPTER II

RESPONSIBILITIES AND AUTHORITIES

PART A - HEADQUARTERS

1. SECRETARY.

   a. Originally classifies NSI up to and including Top Secret.

   b. Delegates Top Secret Original Classification Authority to those principal subordinates who frequently need to exercise such authority.

   c. Requests interpretations of Executive Order 12356 from the Attorney General for any question arising in the course of its administration pursuant to section 6.2(b) of Executive Order 12356.

2. ASSISTANT SECRETARY FOR DEFENSE PROGRAMS.

   a. Approves basic DOE policy on the classification and declassification of RD, FRD, and NSI; approves the "Classification Policy Guide for Nuclear Programs" and other formal statements of DOE classification policy.

   b. Declassifies and transclassifies RD and declassifies FRD in accordance with sections 142(a), (c), (d), and (e) of the Atomic Energy Act.

   c. Assures DOE implementation of the classification and declassification provisions of the Atomic Energy Act and Executive Order 12356.

   d. Determines which categories of information, in addition to those in section 1.3(a) of Executive Order 12356, are related to the national security and require protection against unauthorized disclosure.

   e. Grants and revokes waivers of the requirement to portion mark documents containing NSI only.

   f. Grants and revokes waivers of the requirement to prepare classification guides in areas concerning NSI for specified classes of documents and information.

3. DEPUTY ASSISTANT SECRETARY FOR INTELLIGENCE.

   a. Serves as the Senior Official of the Intelligence Community for DOE.

   b. Advances the application of uniform procedures for administrative handling and accountability of Sensitive Compartmented Information (SCI), including the classification and marking of SCI documents and materials.

4. DEPUTY ASSISTANT SECRETARY FOR SECURITY AFFAIRS.

   a. Oversees the implementation of the classification and declassification provisions of the Atomic Energy Act and Executive Order 12356.

   b. Reclassifies NSI previously declassified and disclosed, in accordance with section 1.6(c) of Executive Order 12356.

5. DIRECTOR OF CLASSIFICATION.

   a. General Responsibilities and Authorities.

      (1) Develops (for the approval of DP-1) the "Classification Policy Guide for Nuclear Programs" and other formal statements of DOE classification policy; coordinates proposed policies with appropriate DOE program organizations.

      (2) Interprets DOE classification policy.

      (3) Develops and implements DOE classification and declassification rules, regulations, and procedures.

      (4) Recommends to DP-1 all actions for removing information from the RD and FRD categories.

      (5) Determines the proper classification category and level of DOE information; interprets what information falls within the RD definition.

      (6) Manages the DOE Classification Guide System.

         (a) Assures the preparation, coordination, and issuance of classification guidance for DOE programs that involve or generate classified information.

         (b) Coordinates and assures issuance of classification guidance for classified information generated under the cognizance of DOE when the classification policy for such information is developed by other Government agencies or foreign governments.

         (c) Approves all program classification guides prior to their issuance. Approves local classification guides or delegates authority for their approval to field elements, as appropriate.

         (d) Conducts a continuing review of all DOE classified information and classification guides to ensure their accuracy and currency and to identify which information may be declassified without undue risk to the common defense and security.

(e) Maintains an index of all DOE and DOE contractor classification guides.

(7) Oversees international classification cooperation.

(a) Maintains liaison and serves as DOE contact with foreign governments on matters concerning classification and declassification of information.

(b) Develops classification and declassification standards as required for international agreements for cooperation entered into pursuant to the provisions of the Atomic Energy Act, and reviews and evaluates foreign classification and declassification policies, procedures, and actions established or taken pursuant to such agreements to assure that they are consistent with the requirements of the agreements.

(8) Manages programs for the classification and declassification review of documents and other materials.

(a) Performs final reviews of all classified documents requested from DOE under the provisions of the FOIA; determines the proper classification thereof; if possible, prepares sanitized versions of such documents; and is the DOE Denying Official with regard to the denial of classified information requested pursuant to the FOIA.

(b) Reviews all testimony, transcripts, and other documents prepared for the Congress in potentially classified subject areas and, as requested, documents prepared by Congress dealing with DOE-related programs involving classified information or where any uncertainty may exist concerning the classification of such documents.

(c) Reviews documents for classification and declassification submitted by Departmental Elements, DOE contractors, and other Government agencies.

(d) Reviews patent applications in potentially classified subject areas.

(e) Reviews documents submitted by uncleared authors.

(f) Assists the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by reviewing classified documents containing DOE information that are proposed for inclusion in the FRUS series.

(9) Advises system managers with regard to classified documents requested pursuant to the Privacy Act of 1974.

(10) Conducts a continuous review of the classification and declassification program to ensure compliance with the classification provisions of the Atomic Energy Act, Executive Order 12356, and this Order.

(11) Develops classification and declassification education and training programs, and administers such programs for the HQ personnel and, as required, field element personnel.

(12) Advises and assists Heads of Departmental Elements with regard to classification and declassification policies and procedures and changes thereto.

(13) Approves field elements' requests to conduct large-scale declassification reviews. Approves specific procedures for such reviews at Headquarters.

(14) Appraises the effectiveness of the classification functions of Departmental Elements.

(15) Obtains service of field elements, contractor personnel, or private consultants, when necessary, in the classification and declassification program.

(16) Approves, after coordination with the appropriate Headquarters Element, a procedure for discharging classification and declassification responsibilities and authorities related to its Headquarters-administered contracts.

(17) Maintains liaison and serves as the DOE contact with other Government agencies and private interests on matters concerning DOE classification and declassification policies and procedures and, as appropriate, provides classification and declassification guidance and training.

(18) Performs other functions assigned by DP-1.

b. Responsibilities and Authorities Derived From Executive Order 12356.

(1) Acts as the Senior Agency Official responsible for the direction and administration of the DOE information security program, except for those provisions of the Executive Order and implementing directives which deal with the safeguarding of classified information such as personnel security, physical security, and the establishment of special access programs.

(2) Originally classifies NSI information as Top Secret, Secret, or Confidential (Executive Order 12356, section 1.2(d)(2)).

(3) Publishes in the "Federal Register" those parts of DOE classification regulations which implement Executive Order 12356 and affect members of the public.

(4) Makes recommendations to DP-1 with regard to the determination of categories of information related to national security and requiring protection against unauthorized disclosure pursuant to section 1.3(a)(10) of Executive Order 12356; ensures that such determinations are reported to the Information Security Oversight Office (ISOO).

(5) Declassifies NSI on a Departmentwide basis, consistent with established DOE classification policy.

(6) Represents the Secretary in any interagency meetings convened by the ISOO; acts as the DOE contact with the ISOO; and advises the Secretary and DP-1 with regard to actions and determinations made by the Director of the ISOO affecting DOE.

(7) Collects, prepares, and submits information to the ISOO pursuant to Executive Order 12356, its implementing directives, and requests of the ISOO.

(8) Makes recommendations to the Secretary concerning the designation of certain Top Secret Classifiers; acts for the Secretary in designating other Top Secret Classifiers, all Original Secret and Confidential Classifiers, and all HQ Derivative Classifiers.

(9) Notifies the Director of Safeguards and Security (DP-34) of the appointment of Top Secret Classifiers so that DP-34 may assign appropriate Top Secret authenticating symbols.

(10) Monitors the requirements for and use of original classification authority in DOE and DOE contractor organizations.

(11) Acts for the Secretary in designating Derivative Declassifiers and maintains a record of all DOE and DOE contractor Derivative Declassifiers.

(12) Issues, reviews, and updates guidelines for systematic declassification review and designates experienced personnel to assist the Archivist of the United States in the conduct of systematic reviews of information originated by DOE.

(13) Conducts, as required, an internal systematic review program for classified information originated by DOE.

(14) Develops procedures to process requests for the mandatory review of NSI and publishes in the "Federal Register" the Departmental Element to which such requests may be addressed.

(15) Serves as the central DOE authority for receiving all requests for declassification review of information under the mandatory review provisions of Executive Order 12356.

(16) Exercises, as necessary, the authority granted by section 1.6(d) of Executive Order 12356 to classify documents requested pursuant to the FOIA or the mandatory review provisions of Executive Order 12356.

6. HEADS OF HEADQUARTERS ELEMENTS.

a. Establish internal procedures to assure compliance with this Order and any other regulations or instructions issued by the Office of Classification.

b. Appoint, if so requested by DP-32, an individual (Headquarters Classification Representative) to be responsible for liaison with the Office of Classification.

c. Request designations of classification authority as needed for HQ Elements or contractors under their jurisdiction.

d. Assure participation by personnel with classification responsibility in the planning stages of new programs that have potential for involving or generating classified information.

e. Inform DP-32 of all proposed projects or HQ-administered contracts that could involve classified information so that DP-32 may assure that appropriate and adequate classification guidance is available for such projects or contracts.

f. Establish, with the approval of DP-32, procedures to carry out an appropriate classification program for HQ-administered contracts.

g. Assure that DOE and DOE contractor personnel within their jurisdiction who publish or deliver papers at conferences or any other presentation concerning potentially classified subject areas are informed by classification representatives on existing classification guidance in the subject areas of their papers and advised as to potential danger areas in the discussion following their presentations.

h. Assure appropriate classification review of all documents or materials prepared by DOE or DOE contractor personnel under their jurisdiction concerning potentially classified subject areas.

i. Assist DP-32 in preparing program classification guides or revisions thereto.

j. Obtain classification guidance from DP-32 for programs under their purview that have a potential for involving or generating classified information; assure that all employees in their HQ element or contractors under their jurisdiction receive adequate classification guidance for their work.

k. Assure that approved classification guidance is included with authorization of new work initiated by their HQ element when such work is likely to involve or generate classified information.

l. Provide DP-32 with information required to be maintained by DP-32 or reported to the ISOO in accordance with Executive Order 12356 and its implementing directives, or as determined to be required by DP-32.

m. Establish, when necessary, detailed procedures for large-scale declassification reviews and submit such procedures to DP-32 for approval.

n. Assist DP-32 in the classification education program for HQ Elements and their contractors.

o. Assist DP-32 in the classification appraisal program of HQ Elements and contractors involved with classified information; follow up on appraisal findings requiring corrective action; take action on recommendations made in appraisals of the classification programs under their supervision; ensure that major prime contractor organizations conduct classification appraisals of subcontractor organizations involved with classified information.

p. Take appropriate and prompt corrective action whenever a classification violation occurs within their organizations.

7. HEADQUARTERS CLASSIFICATION REPRESENTATIVES.

a. Serve as the point-of-contact for their elements with DP-32 concerning classification policies and procedures.

b. Assist the Heads of HQ Elements in exercising their classification and declassification responsibilities and authorities.

c. Respond to questions from individuals within their elements concerning classification policies and procedures and refer questions, as necessary, to DP-32.

d. Maintain a current listing of Authorized Classifiers and Derivative Declassifiers within their elements.

8. DEPARTMENT OF ENERGY EMPLOYEES.

a. Refer questions concerning classification or declassification of information, documents, or material to Authorized Classifiers, their classification office, or through channels to DP-32.

b. Obtain a determination from an Authorized Classifier on information, documents, or material the classification of which is in question.

c. Refer suggestions, complaints, or challenges concerning the DOE classification and declassification program to their classification office or DP-32.

PART B - FIELD ELEMENTS AND CONTRACTOR ORGANIZATIONS

1. HEADS OF FIELD ELEMENTS.

   a. Establish internal procedures to assure compliance with provisions of this Order and any other regulation or instruction issued by DP-32.

   b. Designate, when needed and with the concurrence of DP-32, persons to serve as DOE Classification Officers. Review contractor nominations for Classification Officers and recommend DP-32 approval.

   c. Request of DP-32, as needed for field elements or contractors under their jurisdiction, designations of classification authority for:

      (1) Original Classification Authority (all levels);

      (2) Top Secret Derivative Classification Authority; and

      (3) Derivative Declassification Authority.

   d. Assure designation of Secret and Confidential Derivative Classifiers, as necessary, for field elements or contractors under their jurisdiction and maintain a listing of such classifiers and declassifiers in field elements and contractors under their jurisdiction.

   e. Assure participation by appropriate Classification Officers and other personnel with classification responsibility in the early planning stages of new programs that have potential for involving or generating classified information.

   f. Obtain classification guidance from DP-32 for programs under their purview that concern potentially classified subject areas.

   g. Assist DP-32 in preparing program classification guides or revisions thereto.

   h. Assure that field elements and contractors under their jurisdiction prepare local classification guides or receive program classification guides approved for this purpose covering all classified work being performed.

      (1) Where delegated such authority, approve local classification guides for implementation, providing final copies for the record to DP-32.

      (2) Where local approval authority has not been delegated, submit proposed local classification guides and significant changes in local classification guides to DP-32 for approval prior to their issuance.

i. Assure that approved classification guidance is included with authorization of new work initiated by field elements or contractors under their jurisdiction when such work is likely to concern classified subject areas, and provide copies of such guidance to DP-32 at the time of initial distribution.

j. Assure that DOE and contractor personnel within their jurisdiction who publish or deliver papers at conferences or any other presentation concerning potentially classified subject areas are informed by classification representatives on existing classification guidance in the subject areas of their papers and advised as to potential danger areas in the discussion following their presentations.

k. Assure that all documents and materials prepared within their jurisdiction by DOE or DOE contractor personnel concerning potentially classified subject areas receive appropriate classification review.

l. Provide DP-32 with information required to be maintained by DP-32 or reported to the ISOO in accordance with Executive Order 12356 and its implementing directives, or as determined to be required by DP-32.

m. Establish, when necessary, detailed procedures for special large-scale reviews of accumulations of classified documents in their field elements. Approve such plans when submitted by contractors under their jurisdiction, after consultation with DP-32.

n. Develop and conduct a classification appraisal program for their field elements and contractors involved with classified information; follow up on appraisal findings requiring corrective action; take action on recommendations made in appraisals of the classification programs under their supervision; ensure that major prime contractor organizations conduct classification appraisals of subcontractor organizations involved with classified information.

o. Take appropriate and prompt corrective action whenever a classification violation occurs within their field elements.

p. Assure that an appropriate classification education program is conducted for DOE and DOE contractor organizations under their jurisdiction.

q. Appoint Classification Boards, as appropriate.

r. Assure that Heads of contractor organizations discharge, in relation to their own organization, subcontractors and suppliers, the responsibilities and authorities specified in (a) through (q), above, by including appropriate provisions in their contracts. If these responsibilities entail submission of information to DP-32, it should be made through the appropriate Headquarters or field element.

2. FIELD ELEMENT AND CONTRACTOR CLASSIFICATION OFFICERS.

a. Assist or act for the Head of their Field Element or contractor organization, as appropriate, in exercising their responsibilities and authorities with regard to classification and declassification.

b. Maintain continuous contact with appropriate technical staff personnel and with other Classification Officers in related programs.

c. Provide classification guidance to employees within their organization and, as necessary, to their contractors or subcontractors.

d. Coordinate the preparation of local classification guides for fields of operation or programs within their purview.

e. Assure that DOE and DOE contractor personnel within their jurisdiction who publish or deliver papers at conferences or any other presentation concerning potentially classified subject areas are informed on existing classification guidance in the subject areas of their papers and advised as to potential danger areas in the discussion following their presentation.

f. Assure that all documents and materials prepared by DOE or contractor personnel within their jurisdiction concerning potentially classified subject areas receive appropriate classification review.

g. Provide technical advice, as requested, to DP-32 on classification matters of mutual interest.

h. Initiate classification and declassification reviews of documents originated within their field elements.

i. Conduct classification appraisals of their contractor or subcontractor organizations.

j. Supervise special declassification activities or reviews.

k. Conduct a classification education program for their field elements and assure that such programs are conducted at their contractors' and subcontractors' sites.

l. Appoint Classification Boards, as appropriate.

3. RESPONSIBLE REVIEWERS.

a. Advise DP-32 with regard to the classification of information within their fields of competence.

b. Make recommendations to DP-32 regarding the declassification or continued classification of documents or materials submitted for their review.

4. FIELD ELEMENT AND CONTRACTOR EMPLOYEES.

a. Refer questions concerning classification or declassification of information, documents, or material to Authorized Classifiers, their classification office, or through channels to DP-32.

b. Obtain a determiniation from an Authorized Classifier on information, documents, or material the classification of which is in question.

c. Refer suggestions, complaints, or challenges concerning the DOE classification and declassification program to their classification office or DP-32.

PART C - APPOINTMENTS AND QUALIFICATIONS

1. AUTHORIZED CLASSIFIERS. See Chapter V, Part A.

2. AUTHORIZED DECLASSIFIERS. See Chapter VI, Part A.

3. CLASSIFICATION OFFICERS (FIELD ELEMENT AND CONTRACTOR).

   a. Qualifications. Classification Officers must have a scientific or technical degree unless otherwise approved by DP-32 on a case-by-case basis. Classification Officers will be designated as Authorized Classifiers.

   b. Appointment. Heads of Field Elements shall designate, when needed and with the concurrence of DP-32, persons to serve as Classification Officers. They shall review contractor nominations for Classification Officers and recommend DP-32 approval.

4. HEADQUARTERS CLASSIFICATION REPRESENTATIVES.

   a. Qualifications. Headquarters Classification Representatives shall normally be expected to have the same qualifications as an Authorized Classifier. Exceptions may be granted by DP-32.

   b. Appointment. Headquarters Classification Representatives will be designated by the Heads of Headquarters Elements with the concurrence of DP-32.

5. RESPONSIBLE REVIEWERS.

   a. Qualifications. Responsible Reviewers must be qualified experts who are recognized authorities in their respective fields. They also must be knowledgeable in DOE classification policies and procedures.

   b. Appointment. Responsible Reviewers are appointed by DP-32.

CHAPTER III

POLICY AND OBJECTIVES

1. GENERAL. The objectives of the DOE classification program are the establishment of policies and procedures which ensure the proper classification of information within the purview of DOE requiring protection in the interest of the security of the United States, and the identification of those documents and materials which reveal such information so as to assure its protection. Information within the purview of the DOE classification program includes RD and FRD, which are classified at their inception pursuant to the Atomic Energy Act, and NSI, which is classified pursuant to Executive Order 12356.

2. RESTRICTED DATA AND FORMERLY RESTRICTED DATA.

   a. Pursuant to the Department of Energy Organization Act and the Energy Reorganization Act of 1974, as amended, the Secretary of Energy has certain responsibilities with regard to the control of information which falls under the purview of the Atomic Energy Act. In accordance with the Atomic Energy Act, it is DOE policy to control the dissemination and declassification of RD and FRD in such a manner as to assure the common defense and security. Consistent with such policy, DOE shall be guided by the following principles (section 141, Atomic Energy Act):

      a. Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 144; and

      b. The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information.

   b. It is DOE's responsibility, through DP-32, to interpret and implement the classification and declassification provisions of the Atomic Energy Act. (See Chapter X, Part A for excerpts from the Atomic Energy Act.)

3. NATIONAL SECURITY INFORMATION.

   a. Pursuant to Executive Order 12356 (see Chapter X, Part B) and the Presidential Order of 5-7-82, "National Security Information," the Secretary of Energy has certain responsibilities with regard to the

control of information which falls under the purview of DOE and which may be classified as NSI. It is DOE policy:

(1) To classify as NSI, in accordance with the provisions of Executive Order 12356, information concerning the national defense and foreign relations of the United States which, in the interests of the United States and its citizens, must be protected against unauthorized disclosure.

(2) That only individuals specifically authorized to do so may originally classify or declassify information or derivatively classify or declassify documents or other material.

(3) That, whenever possible, all classified information be covered by classification guides approved by DP-32.

b. It is DOE's responsibility, through DP-32 and DP-34, to interpret and implement Executive Order 12356 as it applies to information under the purview of DOE.

4. LIMITATIONS ON CLASSIFICATION OF NATIONAL SECURITY INFORMATION.

a. Classification may not be used to conceal violations of the law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; or to restrain competition.

b. Basic scientific research information not clearly related to the national security may not be classified.

c. Classification may not be used to limit dissemination of information that is not classifiable or to prevent or delay the public release of such information.

5. CLASSIFICATION OF FOREIGN GOVERNMENT INFORMATION. Foreign government or international organization of governments information shall either retain its foreign government classification designation or be assigned a U.S. classification category, level, and duration equivalent to that assigned by the foreign government or international organization that furnished the information. Documents or other material containing or revealing foreign government information shall be derivatively classified on the basis of the source document from which the foreign government information was extracted, or, if available, guidance covering the subject. Special security markings are required on such documents. Refer to DOE 5635.1, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, for detailed marking instructions. If information given "in confidence" by another government is not marked as classified when received, a determination to classify shall be made in accordance with guidance provided by DP-32.

6. CHALLENGES TO CLASSIFICATION. Those involved with classified information are encouraged to challenge the classification of information, a document, or material when there is reason to believe that it is classified unnecessarily, improperly, or for an inappropriate period of time. Those who wish to make such a challenge should, under normal circumstances, request that those responsible for such classifications reexamine their determinations. If satisfactory resolutions are not reached, or if the challengers do not wish to challenge the classifiers directly, they may take the matter to higher authority for resolution.

CHAPTER IV

CLASSIFICATION CRITERIA AND LEVELS

PART A - CRITERIA FOR CLASSIFICATION

1. RESTRICTED DATA AND FORMERLY RESTRICTED DATA. Information under the purview of the Atomic Energy Act is classified at its inception by that Act. There is no original determination required to classify such information because all RD and FRD is originally classified by the Act.

2. NATIONAL SECURITY INFORMATION.

   a. Criteria for Classification. The following two conditions must be met before official information may be classified pursuant to Executive Order 12356:

      (1) The information must concern at least one of the following areas:

         (a) Military plans, weapons, or operations;

         (b) Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

         (c) Foreign government information;

         (d) Intelligence activities (including special activities) or intelligence sources or methods;

         (e) Foreign relations or foreign activities of the United States;

         (f) Scientific, technological, or economic matters relating to the national security;

         (g) U.S. Government programs for safeguarding nuclear materials or facilities;

         (h) Cryptology;

         (i) A confidential source; or

         (j) Other categories of information related to the national security that require protection against unauthorized disclosure, as determined by the President, the Secretary of Energy, or DP-1. Any determination made under this subsection shall be reported promptly to the Director of ISOO by DP-32.

      (2) The unauthorized disclosure of the information itself or in the context of other information could reasonably be expected to cause damage to the national security. (Note: Unauthorized disclosure of foreign government information, the identity of a confidential

foreign source, or intelligence sources or methods is presumed by Executive Order 12356 to cause damage to the national security.)

b. Unofficial Publication or Inadvertent or Unauthorized Disclosure. Information classified in accordance with the above shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

PART B - LEVEL OF CLASSIFICATION

1. CLASSIFICATION LEVELS. The designations used to specify levels of protection for RD, FRD, and NSI are as follows, in descending order of sensitivity:

   a. Top Secret shall be used only for information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

   b. Secret shall be used only for information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

   c. Confidential shall be used only for information the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

2. USE OF THE TERM "UNCLASSIFIED". Only the three foregoing designations can be used to identify the level of classified information. The term "unclassified" is used to indicate information that is not classified pursuant to an executive order or a statute. Unclassified information normally is not marked as such except to distinguish it from classified information in a classified document when such a distinction is required or serves a useful purpose. Wholly unclassified documents or materials normally need not be marked "unclassified" unless such a marking would serve a useful purpose. Note: Certain unclassified documents may require additional markings, for example, Unclassified Controlled Nuclear Information (UCNI).

3. CLASSIFICATION IN CONTEXT. Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation which, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

CHAPTER V

CLASSIFICATION OF INFORMATION AND DOCUMENTS

PART A - CLASSIFICATION AUTHORITIES

1. TYPES OF CLASSIFICATION AUTHORITY. There are two basic types of classification authority.

   a. Original Classification Authority applies to information, independent of its medium or form. Original classification applies only to NSI because RD and FRD are "born classified" under the Atomic Energy Act. Original Classification Authority allows an authorized individual to make the initial determination that previously unclassified information should be classified. An original classification decision should not be made when classification guidance exists.

   b. Derivative Classification Authority applies to documents or other material, not directly to the information contained in or revealed by the document or material. It allows an authorized individual to make a determination that a document or other material contains or reveals information that is in substance the same as information already classified. Derivative classification is based on explicit instructions found in formal classification guides, implicit guidance (by example) found in classified source documents, or on instructions from an Original Classifier that a document contains NSI. An individual with Original Classification Authority may also classify documents and other material on a derivative basis. Derivative classification applies to documents or other material containing or revealing RD, FRD, or NSI.

   c. All classification authority is granted to a particular individual in a particular position. Classification authority is not automatically transferred with an individual when transferring to a different position. By the same token, an individual assuming a position previously held by an authorized classifier or acting in that position may not automatically assume classification authority.

   d. Any individual may temporarily mark and protect a questionable document as RD, FRD, or NSI. However, the document must be promptly referred to an appropriate classification authority for final determination.

2. ORIGINAL CLASSIFICATION AUTHORITY.

   a. Restricted Data and Formerly Restricted Data. Individuals do not have Original Classification Authority for RD or FRD. All RD and FRD is originally classified by the Atomic Energy Act.

   b. National Security Information. Original classification is an initial determination by an authorized individual that certain previously unclassified information requires, in the interest of

national security, protection against unauthorized disclosure, together with specification of a classification level (Top Secret, Secret, Confidential) signifying the degree of protection required and the duration of classification. Such a determination can only be made by an Original Classifier pursuant to Executive Order 12356. Information so classified is NSI.

c. Qualifications. An Original Classifier must (1) have demonstrated competence in the subject area in which the authority will be used; (2) be knowledgeable in DOE classification policy and procedures (especially with all classification guides in the subject area in which the authority will be used); (3) be in a position with a proven or anticipated need for Original Classification Authority; and (4) be so designated in writing by appropriate authority as described below.

d. Designation.

(1) Requests for Original Classification Authority for positions that do not currently have such authority should be submitted in writing to DP-32. Such requests should include (1) the level (Top Secret, Secret, Confidential) of Original Classification Authority requested; (2) the name and title of the individual for whom the authority is being requested; (3) a description of the subject area and jurisdiction for which the authority is needed; (4) the anticipated frequency of use of the authority; (5) the effective date of the authority; and (6) any other information which would support the need for such authority and the qualifications of the individual for whom the authority is being requested.

(2) When an individual vacates a position for which Original Classification Authority has been granted, the name and title of the individual losing the authority and the effective date of the loss of the authority must be sent by the individual's organization to DP-32.

(3) When an individual assumes a position for which Original Classification Authority has already been granted, that individual's name, title, and qualifications must be submitted to DP-32 for approval. The individual may not assume the classification authority of the position until his or her approval by DP-32.

(4) Original Classification Authority may not be redelegated.

e. Cancellation.

(1) If the Head of a Departmental Element determines that a position no longer requires Original Classification Authority, DP-32 shall be promptly notified of the position title, the name of the person who holds or last held the position, and the effective date of cancellation of authority.

(2) If DP-32 determines that an individual no longer requires Original Classification Authority, he or she shall advise the person concerned that such authority is to be cancelled, the date of cancellation, and the reasons for the cancellation.

f. Recordkeeping Requirements. DP-32 shall maintain a list of all individuals with Original Classification Authority. This list shall include (1) the level of the authority granted, (2) the name and title of the individual granted the authority, (3) the individual's Departmental Element or contractor organization, and (4) the effective date of the designation. In addition, each Departmental Element and contractor organization shall maintain a similar list of all individuals with Original Classification Authority within their jurisdiction.

g. Authority Definition. (See also Chapter X, Part C.) An individual with Original Classification Authority may:

(1) Originally classify NSI within the classifier's programmatic jurisdiction at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority whenever classification guidance or relevant classified source documents are not available. Such determinations must be consistent with established DOE classification policy. Original Classification Authority does not apply to RD or FRD. See Chapter X, Part D for a detailed analysis regarding making an original classification determination.

(2) Originally declassify or downgrade NSI (except formal reports) from any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority over which the classifier has sole programmatic jurisdiction and which the classifier, his or her predecessors, or their subordinates originally classified, so long as such action is consistent with DOE classification policy and guidance. Original declassification or downgrading authority does not apply to RD or FRD. Refer to page VI-9, paragraph 4 for a more detailed description of Original Declassification/Downgrading Authority.

(3) Derivatively classify documents which contain RD, FRD, and/or NSI as defined in his or her letter of appointment at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority. Such determinations shall be based on classification guides authorized for the classifier's use or on classified source documents. Refer to page V-4, paragraph 3 for a more detailed description of Derivative Classification Authority.

(4) Derivatively declassify or downgrade documents (except formal reports) which the classifier, his or her predecessors, or their subordinates originally or derivatively classified from any

classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority. Such determinations shall be based on classification guides authorized for the classifier's use. Derivative declassification or downgrading authority is applicable to all documents marked as containing any category of classified information (RD, FRD, or NSI). Refer to page VI-1, paragraph 2a, for a more detailed description of Derivative Declassification/Downgrading Authority.

3. DERIVATIVE CLASSIFICATION AUTHORITY.

a. Applicability. Individuals with Derivative Classification Authority may classify documents or other material that contains or reveals RD, FRD, or NSI.

b. Qualifications. A Derivative Classifier must (1) have demonstrated competence in the subject area in which the authority will be used; (2) be knowledgeable in DOE classification policy and procedures (especially with all classification guides in the subject area in which the authority will be used); (c) be in a position with a proven or anticipated need for Derivative Classification Authority; and (d) be so designated in writing, as described below.

c. Designation.

(1) Headquarters. DP-32 appoints all Derivative Classifiers within Headquarters Elements, including contractors under the direct purview of a Headquarters Element.

(a) Requests for Derivative Classification Authority for positions currently without such authority should be submitted in writing to DP-32. Such requests should include (1) the level (Top Secret, Secret, Confidential) of Derivative Classification Authority requested; (2) the name and title of the individual for whom the authority is being requested; (3) a description of the subject area and jurisdiction for which the authority is needed; (4) the anticipated frequency of use of the authority; (5) the effective date of the authority; and (6) any other information which would support the need for such authority and the qualifications of the individual for whom the authority is requested.

(b) When an individual vacates a position for which Derivative Classification Authority has been granted, the name and title of the individual losing the authority and the effective date of the loss of the authority must be sent by the individual's Departmental Element to DP-32.

(c) When an individual assumes a position for which Derivative Classification Authority has already been granted, that

individual's name, title, and qualifications must be submitted to DP-32 for approval. The individual may not assume the classification authority of the position until his or her approval by DP-32.

(2) Field. Each Operations Office is responsible for the establishment of a system to appoint Derivative Classifiers in the field elements and contractor organizations under its purview.

(3) Derivative Classification Authority may not be redelegated.

d. Cancellation.

(1) If the Head of a Departmental Element or contractor organization determines that a position no longer requires Derivative Classification Authority, he or she shall promptly notify the appointing official (e.g., DP-32 for HQ) of the position title, the name of the person who holds or last held the position, and the effective date of cancellation of authority.

(2) If the appointing official (e.g., DP-32 for HQ) determines that an individual no longer requires Derivative Classification Authority, the appointing official shall advise the person concerned of the cancellation of such authority, the date of cancellation, and the reasons for the cancellation.

e. Recordkeeping Requirements. Each appointing official shall maintain a list of all individuals with Derivative Classification Authority under his or her purview. This list shall include (1) the level of the authority granted, (2) the name and title of the individual granted the authority, (3) the individual's Departmental Element or contractor organization, and (4) the effective date of the designation.

f. Reporting Requirements. Each Operations Office shall report annually as part of the "Annual Statistical Report for Information Security Oversight Office" the number of Derivative Classification Authorities, at each level, appointed in Departmental Elements and contractor organizations under its purview.

g. Authority Definition. (See also Chapter X, Part C). Individuals with Derivative Classification Authority may derivatively classify documents or materials which contain RD, FRD, and/or NSI as defined in their letters of appointment at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority. Such determinations shall be based on classification guides authorized for the classifier's use or on classified source documents. See Chapter X, Part E for a detailed analysis on making derivative classification determinations.

PART B - CLASSIFICATION GUIDANCE

1. TYPES OF CLASSIFICATION GUIDANCE. A hierarchy of documents provides classification guidance within DOE. These documents range from the "Classification Policy Guide for Nuclear Programs," approved by DP-1, to local classification guides written by DOE field elements and contractor organizations.

   a. "Classification Policy Guide for Nuclear Programs."

      (1) Originator/Source of Authority. This document is developed by DP-32 for approval by DP-1.

      (2) Purpose. This document is the mechanism by which DP-1 approves basic DOE policy statements on the classification and declassification of all DOE nuclear-related information. It identifies general subject areas under the purview of the Atomic Energy Act that remain classified or have been declassified pursuant to section 142 of that Act. It also identifies certain subject areas related to DOE nuclear programs that are classified as NSI pursuant to Executive Order 12356. Further, this document explains the factors affecting the decision on whether or not a subject area should be classified.

      (3) Users. DP-32 interprets this document when approving program and local classification guides, preparing program guides, or determining that information is unclassified. This guide is not to be used by others for classification/declassification determinations except to the extent expressly delegated by DP-32.

   b. "Guide to the Declassified Areas of Nuclear Energy Research."

      (1) Originator/Source of Authority. This guide is developed and issued by DP-32.

      (2) Purpose. This guide identifies nuclear-related subject areas under the purview of DOE that fall within the definition of RD but have been removed from the category pursuant to section 142a of the Atomic Energy Act. It elaborates on the "Classification Policy Guide for Nuclear Programs."

      (3) Users. Any originator of a document may use this guide to verify that the information in question has been declassified. Detailed instructions as to the scope, use, and limitations of this guide are found in the guide itself.

c. Program Classification Guides.

(1) Originator/Source of Authority. These guides implement the Classification Policy Guide for Nuclear Programs" and other formal statements of DOE policy. Program guides are approved by DP-32 (together with appropriate officials in other Government agencies if the guide is a joint guide).

(2) Purpose. These guides identify specific elements of information under the purview of DOE that are classified or unclassified. Such guides also specify the proper classification level of the specific classified information identified within them and, for NSI, the duration of its classification.

(3) Users. These guides are used by Original and Derivative Classifiers as the basis for their derivative classification determinations and by Derivative Declassifiers as the basis for their derivative declassification determinations. Classifiers may use only those guides approved for their use. Such guides are also used by local classification offices as the basis for preparation of detailed classification guides primarily intended for use within a field or contractor organization.

d. Classification Bulletins.

(1) Originator/Source of Authority. The originator and the source of authority are the same as for program classification guides except that bulletins also may be based on program classification guides.

(2) Purpose. In general, the purpose of classification bulletins is the same as for program classification guides, but with a more limited scope. Most bulletins address specific facts or concepts, whereas a program classification guide typically addresses an entire subject area. Bulletins may interpret, clarify, or expand on guidance contained in a program classification guide. In addition, classification bulletins may be used to promulgate changes in classification procedures.

(3) Users. Bulletin users are the same as those for program classification guides.

e. Local Classification Guides.

(1) Originator/Source of Authority. These guides are based on program classification guides and classification bulletins. Heads of Field Elements and contractor organizations are responsible for assuring that local classification guides are prepared as needed for all classified work within their jurisdictions. Except where approval authority has been specifically delegated to field elements, such

guides must be submitted to DP-32 for review and approval before the originating element uses or issues them. If the responsibility of more than one field element or of another Government agency (such as DOD) or of a foreign government is involved, DP-32 may determine that a local classification guide should be issued as a program classification guide.

(2) Purpose. These guides have the same purpose as program classification guides, but are more detailed and tailored to the specific needs of the originating field element or contractor.

(3) Users. These guides are used by Original and Derivative Classifiers as the basis for their derivative classification determinations and by Derivative Declassifiers as the basis for their derivative declassification determinations. Classifiers may use only those guides approved for their use. Unless otherwise directed by DP-32, local classification guides may be disseminated to other organizations within and outside DOE as required, in accordance with "need-to-know" principles.

2. USE OF PROGRAM AND LOCAL CLASSIFICATION GUIDES.

a. General. Classification guides are to be used wherever they exist. Use of these guides often entails difficult judgments and interpretations of topics. Classifiers or Declassifiers may use only those classification guides specifically approved for their use by their local classification office or by DP-32. Omission from any classification guide of an explicit statement concerning classification of a specific fact within the subject area covered by the guide does not mean that the fact in question is unclassified. In cases in which a guide appears ambiguous, incomplete, or in apparent contradiction to another guide, the local classification office should be consulted for further guidance, and, if needed, referral may be made to DP-32. Pending resolution of the problem, the most restrictive interpretation of the guide should be used.

b. Classification Level/Category. These classification guides indicate the classification level or range of levels and the classification category of specific information within the scope of the subject area of the guide.

c. Duration of Classification. For NSI only, a guide indicates how long specific information must remain classified. This duration can be defined as a period of time measured from the date of origination of the document under review or as an event which must occur prior to declassification. When a specific date or event cannot be determined at the time the classification guide is issued, the declassification instructions will indicate that the "Originating Agency's Determination (is) Required" (OADR). Documents containing RD or FRD, regardless of whether they contain NSI, are not to be marked in advance for declassification.

d. Other Information. These classification guides also contain instructions concerning when and how to use and interpret the guides.

3. CONVERSION OF DECLASSIFICATION AND REVIEW DATES. Refer to page VI-5, paragraph 2, for instructions on how to interpret the declassification and review instructions found in classification guides issued pursuant to Executive orders preceding Executive Order 12356.

4. REQUIREMENT FOR PERIODIC REVIEW OF CLASSIFICATION GUIDES. Those portions of DOE program and local classification guides and bulletins which contain classification guidance for NSI, regardless of whether they also contain classification guidance for RD or FRD subject areas, shall be reviewed for currency and completeness by the issuing office at least every 2 years and updated as necessary.

5. DISTRIBUTION OF LOCAL GUIDES TO DIRECTOR OF CLASSIFICATION. A minimum of three copies of the final version of each local classification guide and all subsequent changes issued by any DOE field element or contractor organization shall be sent to DP-32 as part of the initial distribution of the guide. These copies will be put into (a) the permanent file, (b) the reference file, and (c) the automated Classification Guidance System. Additional copies of such guides may be requested by DP-32, on a case-by-case basis, for use within HQ.

6. INDEX OF CLASSIFICATION GUIDES. DP-32 shall maintain a list of all DOE and DOE contractor classification guides in current use.

7. CLASSIFICATION GUIDANCE FOR WORK NOT FUNDED BY THE DEPARTMENT. Classification guidance for work conducted at DOE facilities but not funded by DOE is the responsibility of the funding organization. The classification guidance so provided will be followed unless it is in conflict with DOE guidance. All conflicts will be reported to DP-32 for resolution. Until resolution, the information in question shall be classified in accordance with the most restrictive guidance.

8. CLASSIFICATION GUIDANCE FOR JOINTLY FUNDED WORK. Classification guidance for work conducted at DOE facilities funded by both DOE and a non-DOE U.S. Government organization is the joint responsibility of both funding organizations. Program offices should contact DP-32 to assure development of appropriate joint classification guidance.

PART C - CLASSIFICATION/SECURITY MARKINGS

1. GENERAL.

   a. All authorized classifiers are responsible for ensuring that the necessary classification/security markings are placed on a classified document. These include:

      (1) Classification level;

      (2) Classification category;

      (3) Date of classification;

      (4) Classification authority and/or identity of the classifier;

      (5) Duration of classification, if applicable;

      (6) Office of origin;

      (7) Special markings (if required);

      (8) Documentation information (if Secret or Top Secret); and

      (9) Authentication information for Top Secret documents.

   b. Refer to DOE 5635.1, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, for rules concerning the use, format, and placement of classification/security markings. This Order describes only certain markings related to the classification of a document.

2. CLASSIFICATION AUTHORITY. All classified documents must indicate the source of classification authority which is the basis for the document's classification and/or the identity of the Authorized Classifier of the document. Documents originated by individuals without appropriate classification authority must be reviewed by an Authorized Classifier having the appropriate authority when it is reasonable to expect that the documents contain classified information or when regulations or other requirements apply. Note that the identification of the classifier of a document, as required in the following paragraphs, is not analogous to preparation of a document for someone else's signature; that is, the identity of the actual classifier of a document and his or her Departmental Element should be indicated.

   a. Restricted Data/Formerly Restricted Data. The following rules apply to all classified documents that contain RD or FRD, regardless of whether they also contain NSI.

(1) The classification authority for documents which contain RD or FRD is the Atomic Energy Act. The RD or FRD stamp serves to identify the source of classification authority (but see paragraph (2) below).

(2) Documents which contain RD or FRD are always derivatively classified and may, therefore, be classified by an Original or Derivative Classifier. The "Derivative Classifier" line on the document must be completed with the name and title of the classifier of the document. In those cases where the signer is the Derivative Classifier, the word "signer" may be substituted for the name and position title of the classifier.

b. National Security Information Only. The following rules apply to classified documents that contain only NSI (i.e., they do not contain any RD or FRD).

(1) Originally Classified. If the classification of a document is not based on the use of classified information from other documents or on classification guides, the document must be classified by an Original Classifier. The "Classified by" line on the document must be completed with the name and position title of the Original Classifier. In those cases where the signer is the Original Classifier, the word "signer" may be substituted for the name and position title of the Original Classifier. (Note: Such documents must be portion marked. See page V-15, paragraph 5 for more detailed information.)

(2) Derivatively Classified. If the classification of a document is based on the use of classified information from another document or on a classification guide, the document must be classified by an Original or Derivative Classifier. The "Classified by" line on the document must include the identity of the classification source (e.g., a classification guide or the date and originator of the memorandum that served as the basis for the classification determination). The "Derivative Classifier" line on the document must be completed with the name and title of the classifier of the document. In those cases where the signer is the Derivative Classifier, the word "signer" may be substituted for the name and position title of the classifier.

(3) More Than One Classification Source. If the classification of a document is based on more than one document, classification guide, or Original Classifier determination, the "Classified by" line must include the term "Multiple Sources." The classifier shall include the identification of each classification source, as specified in the previous two paragraphs, with the file or record copy of the document. Otherwise, the rules for classification marking are as specified in the two preceding paragraphs.

3. DURATION OF CLASSIFICATION.

a. Restricted Data/Formerly Restricted Data. Documents that contain RD or FRD (regardless of whether they also contain NSI) are not to be marked for declassification or review. Therefore, such documents do not require a "Declassify on" line.

b. National Security Information Only. Documents that contain only NSI (i.e., they do not contain any RD or FRD) shall be marked for declassification in accordance with the following:

(1) Originally Classified. If the classification of a document is not based on the use of classified information from other documents or on classification guides, the Original Classifier of the document shall set a specific date or event for declassification at the time the information is originally classified, if possible. The "Declassify on" line on the document must be completed with this date or event. When a specific date or event for declassification cannot be determined at the time of original classification, the "Declassify on" line on the document must be completed with the following: "Originating Agency's Determination Required" or "OADR."

(2) Derivatively Classified.

(a) If the classification of a document is based on the use of classified information from another document, the declassification instructions of the source document should be carried forward to the "Declassify on" line of the new document.

1 Documents deriving their classification from a source document classified pursuant to Executive Order 12356 shall carry forward the declassification instructions from the source document.

2 Documents deriving their classification from a source document classified pursuant to predecessors of Executive Order 12356 should be marked for declassification according to the conversion table in Chapter X, Part F. See also page VI-5, paragraph 2.

(b) If the classification of a document is based on instructions in a classification guide, those instructions should be followed.

1 Documents deriving their classification from a classification guide issued pursuant to Executive Order 12356 shall be marked with the latest date or event for declassification specified for the information concerned or with the indication that the "Originating Agency's

Determination (is) Required" (OADR) if this instruction is specified for any information in the document under review.

2 Documents deriving their classification from a classification guide issued pursuant to predecessors of Executive Order 12356 should be marked for declassification according to the conversion table in Chapter X, Part F. See also page VI-5, paragraph 2.

(c) If the classification of a document is derived from a source document or a classification guide which does not specify declassification instructions, the "Declassify on" line should be completed with "OADR."

(d) Documents deriving their classification from more than one classification guide or source document shall be marked with the latest occurring date or event for declassification indicated in the classification guides or source documents, or with "OADR", as appropriate.

4. OBSOLETE MARKINGS. Certain classification or security markings that were once commonly used but are no longer used or currently have a different meaning are defined below. Prior to any use or distribution, old documents marked with these terms shall be reviewed by a classifier or declassifier to determine their current classification status. The markings of such documents shall be changed to show their proper classification. Pending this review, such documents issued in the time periods indicated below shall be safeguarded as Confidential-NSI documents.

a. Restricted. The term "Restricted" is an obsolete classification marking defined in Executive Order 10290 of 9-24-51, which was superseded by Executive Order 10501, of 12-15-53. During and prior to this time, "Restricted" specified a security level less sensitive than "Confidential." Note that "Restricted" is an active classification marking still used by some foreign governments and international organizations.

b. Official Use Only. From 7-18-49 to 10-22-51, the Atomic Energy Commission used the term "Official Use Only" ("OUO") as a security marking equivalent to the term "Restricted" defined in the previous paragraph. (Note: This marking is currently used as a designation for certain sensitive but unclassified information which requires some degree of protection.)

5. PORTION MARKING.

a. In accordance with the provisions of section 1.5(b) of Executive Order 12356, DP-1 granted a waiver of the requirement of that section to portion mark the classes of documents specified below.

(1) Documents which contain both RD or FRD and NSI.

(2) Documents which contain only NSI and which are derivatively classified.

b. Thus, portion marking is required only for NSI-only documents which have been originally classified.

c. This waiver does not pertain to any document containing only RD or FRD. Such information is not under the jurisdiction of Executive Order 12356 and is not portion marked.

d. This waiver was sought because it is the position of DOE that the use of classification guides clearly is a superior method for providing guidance to Derivative Classifiers.

e. If portion marking an originally classified NSI-only document is not practicable, the document shall contain a statement sufficient to identify the information that is classified, the level of such classification, and the information that is not classified. If all portions of a document are classified at the same level, this fact should be indicated by a statement to that effect on the face of the document.

PART D - UPGRADING

1. AUTHORITY TO UPGRADE THE CLASSIFICATION OF INFORMATION AND DOCUMENTS.

   a. Information.

      (1) Restricted Data and Formerly Restricted Data. Only DP-32, DP-1, or a higher authority may upgrade the level of classification of RD and FRD.

      (2) National Security Information. Only DP-32, DP-1, a higher authority, or an Original Classifier may upgrade the classification of NSI, consistent with DOE classification policy. Original Classifiers have authority only over information which they, their predecessors, or their subordinates originally classified.

   b. Documents and Material. Upgrading the classification of documents or material may be authorized only by Original Classifiers or by Derivative Classifiers pursuant to their designated authorities. However, any individual in possession of a document he or she believes should be upgraded, should protect it accordingly and promptly seek guidance from an appropriate classification authority. A change of classification markings on a document to indicate an upgrade may be carried out by custodians of the documents upon receipt of notification from proper authority. If such upgrades are authorized through classification guides, only those authorized to use the classification guides (i.e., Original and Derivative Classifiers, Derivative Declassifiers) may make changes, or direct that changes be made, on documents or material affected by the change. These requirements do not apply to the immediate correction of a misclassification by issuance of a replacement version.

2. PROCEDURES FOR UPGRADING THE CLASSIFICATION OF INFORMATION AND DOCUMENTS.

   a. Notification of Upgrading.

      (1) Information. Written notification of upgrading of the classification of information shall be made by DP-32 and may be in the format of a classification guide or bulletin.

      (2) Documents and Material. Those individuals authorizing the upgrading of documents will ensure that all holders of the documents are notified as follows:

         (a) Content of Notices. Classification upgrading notices should identify the document as fully as possible, citing the title (or briefly describing the document); the identification

number, if any; the author; the document date; the person authorizing the change; and the nature and date of the change. Notices should be classified in accordance with appropriate classification guidance.

(b) Formal Reports. The person authorizing the upgrading of a formal report that has been distributed outside the originating organization shall provide a copy of the upgrading notice to the Office of Scientific and Technical Information, Oak Ridge, Tennessee 37831, for inclusion in that office's data base.

(c) Forwarding of Notices. If the recipient of an upgrading notice has transmitted the document to another custodian, the upgrading notice should be forwarded to the new custodian.

b. Marking of Upgraded Documents. The person changing the markings of a document upon receipt of proper authorization shall mark the new classification on the document and delete the former markings. Any such changes must be verified by a second individual. The following statement shall also be placed on the first page of the document:

Classification changed to

CNSI
(Insert appropriate classification level and category)

by authority of Change Notice #2A (Authority for change in classification) 2/20/80 (Date)

by A.B. Cousins and D.E. Floyd (Signatures of persons making and verifying change) 3/3/81 (Date)

Figure V-1
Example of Upgraded Document Marking

PART E - RECLASSIFICATION

1. AUTHORITY TO RECLASSIFY INFORMATION AND DOCUMENTS.

   a. Information.

      (1) Restricted Data and Formerly Restricted Data. Pursuant to section 146 of the Atomic Energy Act of 1954, as amended, RD and FRD information which has been formally declassified by proper authority may not be reclassified.

      (2) National Security Information. NSI which has been formally declassified by proper authority may only be reclassified by the Deputy Assistant Secretary for Security Affairs (DP-30) or higher authority. Pursuant to section 1.6(c) of Executive Order 12356, previously declassified NSI information may be reclassified if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. (See ISOO Directive No. 1 on pages X-15-22 for further information.)

   b. Documents and Material. In most cases, documents and material may be reclassified by their Original Classifiers or by Derivative Classifiers pursuant to their designated authority. However, only DP-32 or higher authority may reclassify NSI-only documents or material following an FOIA or Privacy Act request. Custodians of the documents may indicate reclassification by changing the classification markings on a document upon receipt of notification from proper authority. If such reclassifications are authorized through classification guides, only those authorized to use the classification guides (i.e., Original and Derivative Classifiers and Derivative Declassifiers) may make changes, or direct that changes be made, on documents or material affected by the change.

2. PROCEDURES FOR RECLASSIFYING INFORMATION AND DOCUMENTS.

   a. Notification of Reclassification.

      (1) Information. Written notification of reclassification of information shall be made by DP-32 and may be in the form of a classification guide or bulletin.

      (2) Documents and Material. Those individuals authorizing the reclassification of documents will assure that all holders of the documents who have a clearance for and a need to know the reclassified information are notified as follows:

         (a) Content of Notices. Reclassification notices should identify the document as fully as possible, citing the title (or

briefly describing the document); the identification number, if any; the authority; the document date; the person authorizing the change; and the nature and date of the change. Notices should be classified in accordance with appropriate classification guidance.

(b) Forwarding of Notices. If the recipient of a reclassification notice has transmitted the document to another custodian who has the proper level of clearance and a need to know the reclassified information, the reclassification notice should be forwarded to the new custodian.

b. Marking of Reclassified Documents. The person changing the markings of a document upon receipt of proper authorization to reclassify it shall mark the new classification on the document and cancel the former markings (if any). Any such change must be verified by a second individual. The following statement shall also be placed on the first page of the document:

Reclassified to CNSI
(Insert appropriate classification level and category)

by authority of Change Notice #2A 2/2/80
(Authority for reclassification) (Date)

by A. B. Cousins and D. E. Floyd 3/3/81
(Signatures of persons making and verifying change) (Date)

Figure V-2
Example of Reclassified Document Marking

PART F - CLASSIFICATION STATUS OF RESEARCH AND DEVELOPMENT ACTIVITIES

1. GENERAL.

   a. Research and development (R&D) conducted under the purview of DOE uses or generates information ranging from completely unclassified to wholly classified. Consistent with the needs of national security, as much of this work as possible is kept unclassified in order to promote the free interchange of ideas essential to scientific and industrial progress and public understanding. All DOE R&D activities must be evaluated to determine the nature and extent of classification requirements applicable to the activities. This review is particularly important in areas of new or rapidly expanding technology. The purpose of this part is to describe (1) the steps involved in making classification status determinations (see Chapter X, Part G), and (2) the resulting requirements imposed upon the program organization. These determinations are based on the potential for generating classified information by the R&D activities. The responsible Heads of HQ or Field Elements will determine what constitutes an R&D "activity" for the purposes of this section. Activities are described as: Category I, unclassified activity with virtually no potential for using or generating classified information; Category II, unclassified activity with the potential for using or generating classified information; and Category III, classified activity with great potential for using or generating classified information.

   b. Since there are two bases for classification of information (the Atomic Energy Act for RD/FRD and Executive Order 12356 for NSI), determination of the classification status of a DOE R&D activity requires the merging of two different but parallel evaluations. The steps involved in this process are described in Chapter X, Part G. Additional procedural guidance is available from DP-32.

2. AUTHORITIES AND REQUIREMENTS FOR DETERMINATION OF RESEARCH AND DEVELOPMENT ACTIVITY CLASSIFICATION STATUS. The following authorities and requirements relate to the determination of the classification status category of DOE R&D activities. (Refer to Chapter X, Part G, Figure X-6).

   a. Determination Authority. Heads of HQ and Field Elements, as appropriate, may designate the classification status category of DOE R&D activities under their programmatic jurisdiction. This determination may be changed by DP-32, who also may permanently or temporarily waive the requirement to make this determination for certain programs.

   b. Reporting Requirements. All category designations shall be reported to the local classification office. Activities with Category II or III designations (see Chapter X, Part G, paragraph 3 and Figure X-6) shall

also be reported annually to DP-32. These reports shall include (1) a description of the activity; (2) the category designation; (3) the name and title of the individual designating the category; (4) the date of the designation; and (5) the name, title, and address of the individual programmatically responsible for the activity (usually the principal investigator).

c. Recordkeeping Requirements. All designations of classification status category of R&D activities shall be recorded and maintained by the local classification office or by the HQ program office, as appropriate. DOE field sites which do not have a local classification office (e.g., Energy Technology Centers) shall have their records maintained by the appropriate HQ program office. The information required in the reports described in the previous paragraph shall be recorded by the local classification office or by the HQ program office, as appropriate, for all DOE R&D activities under their jurisdiction.

d. Appointments. (Refer to Chapter X, Part G, Figure X-6.) Category I activities do not have any appointment requirements. Category II activities require that at least a Derivative Classifier (usually the principal investigator) be designated to monitor the activity to assure that any classified information used or generated by the activity is identified and classified, and that the activity is upgraded to Category III. Category III activities require the appointment of a Classification Officer for the program element (e.g., the overall contractor Classification Officer) or coordination with the responsible Headquarters or field element for classification assistance.

e. Guides are required for Category III activities. In certain circumstances, DP-32 may request the preparation of a classification guide for Category II activities.

PART G - CLASSIFICATION REVIEW OF NEWLY GENERATED DOCUMENTS

1. GENERAL.

   a. The following procedures apply to the classification review of all newly generated documents originated by DOE or its contractors. Variations in the review process are based on the following differences in the types of documents:

      (1) Format;

      (2) Purpose;

      (3) Intended distribution;

      (4) Author's security clearance;

      (5) Author's classification authority; and

      (6) Subject area.

   b. It is DOE policy to provide formal classification guidance whenever possible. However, the absence of a topic in a guide is not sufficient to declare a document unclassified. (Refer to sections below and Chapter V, Part A.)

   c. Determination that a document is unclassified does not mean it can be released to the public. Other factors (e.g., FOIA exemptions such as section 148 of the Atomic Energy Act, Privacy Act exemptions, Patent Secrecy Act, patent clearance review) may limit the releasability of all or part of the document.

2. DOCUMENTS ORIGINATED BY DEPARTMENTAL ELEMENTS OR DEPARTMENTAL CONTRACTOR PERSONNEL. These procedures apply to all documents originated by DOE or DOE contractor personnel. DP-32 and Heads of Field Elements may exempt specific categories of documents or subject areas from these procedures.

   a. Documents Which Concern Category I Activities or which deal with non-R&D subjects having no potential for using or generating classified information do not require classification review by an Authorized Classifier. However, any questionable cases should be referred for review to an Authorized Classifier. (This decision is the responsibility of the originator.)

   b. Documents Which Concern Category II or Category III Activities. All newly generated documents written by DOE or DOE contractor personnel, regardless of their format, that concern Category II or Category III R&D activities or any other subject area having a potential for using or

generating classified information must be reviewed for classification by an Authorized Classifier. Such a review is sufficient for documents that the Authorized Classifier determines (1) to be classified or (2) to be unclassified, but which will receive limited distribution. Examples of such unclassified but limited distribution documents include most letters, memoranda, internal analyses, and planning documents.

c. Documents Intended for Widespread Distribution or Public Release. All newly generated documents written by DOE or DOE contractor personnel, regardless of their format, that concern Category II or Category III program subject areas, or other classified areas and that are intended for public release or for such widespread internal distribution that public release is likely, must be reviewed for classification by the DOE or DOE contractor classification office or DP-32, as appropriate. This authority may be delegated to specified Authorized Classifiers. Examples of this type of unclassified document include formal reports, journal articles, press releases, speeches, and conference papers.

d. Oral Presentations. The review requirements described in subparagraphs a, b, and c, above, are also applicable to any oral presentation, including speeches, briefings, or interviews, to be made by DOE or DOE contractor personnel. Whenever possible, such presentations should be made from a prepared text which has been reviewed according to the applicable requirements described above. When review of prepared text is not possible or when extemporaneous remarks are likely, the person who is to deliver the oral presentation shall be thoroughly briefed beforehand by local DOE or DOE contractor classification office representatives on classification guidance in the field covering the subject matter of the paper and advised of the danger areas in discussions following the presentation.

3. DOCUMENTS SUBMITTED BY PERSONS OTHER THAN DEPARTMENTAL OR DEPARTMENTAL CONTRACTOR PERSONNEL. These procedures apply to documents submitted by persons other than DOE or DOE contractor personnel (a) with past or current DOE security clearances, (b) with past or current security clearances issued by other Government agencies, or (c) with no record of a security clearance.

a. All newly generated documents that concern Category II or Category III DOE R&D activities written by persons other than DOE or DOE contractor personnel possessing an active security clearance from DOE or another agency and submitted for review, are subject to the requirements described in paragraph 2, above. Documents submitted by such individuals for classification review shall be reviewed by the local classification office or DP-32. The author will be requested to delete any classified information contained in the document prior to its unclassified publication.

b. Documents submitted by persons who no longer have a security clearance will normally be treated under the rules of subparagraph 3a, above,

unless the document deals with areas in which they were not authorized access. Those cases should be referred to DP-32.

c. Documents submitted for classification review by persons who never had a security clearance shall be referred to DP-32. The submitter may be notified of this referral, but no further elaboration should be made.

4. REVIEW OF DOCUMENTS (PATENT APPLICATIONS AND REPORTS) REFERRED UNDER SECTIONS 151(c) AND 151(d) OF THE ATOMIC ENERGY ACT.

a. Reports of inventions and discoveries useful in the production and utilization of special nuclear material or atomic energy and concerning Category II or Category III R&D activities shall be forwarded by the Assistant General Counsel for Patents (GC-42) to DP-32 and reviewed to determine whether the reports contain classified information.

b. Patent applications referred to GC-42 by the Commissioner of Patents and Trademarks under section 151(d) of the Atomic Energy Act and forwarded to DP-32 shall be reviewed to determine whether they contain classified information.

c. Both reports of inventions and patent applications shall be handled in accordance with section 151(e) of the Atomic Energy Act, shall be kept in confidence by DOE, and shall not be referred to a Responsible Reviewer for classification review without express written approval of GC-42.

5. WAIVER OF REVIEW REQUIREMENTS. The classification review requirements described in this part may be waived on a case-by-case basis by DP-32.

CHAPTER VI

DECLASSIFICATION AND DOWNGRADING

PART A - AUTHORITY FOR DECLASSIFICATION AND DOWNGRADING

1. INFORMATION.

   a. Restricted Data and Formerly Restricted Data. Only DP-1 may declassify RD and FRD. DP-1 and DP-32 may downgrade RD and FRD.

   b. National Security Information. Declassification and downgrading authority is limited to the Original Classifiers of such information, DP-32, and DP-1.

2. DOCUMENTS AND MATERIAL.

   a. General. Documents and material may be declassified by DP-32, Original Classifiers (see page VI-9, paragraph 4, below, for extent and limitations of such authority), or Derivative Declassifiers. (Note: A custodian of classified documents or material does not require declassification authority in order to proceed in accordance with a declassification notice from an authorized source.)

   b. Derivative Declassification Authority.

      (1) Qualifications. A Derivative Declassifier must (a) have demonstrated competence in the subject area in which the authority will be used; (b) be knowledgeable in DOE classification policy and procedures (especially with all classification guides in the subject area in which the authority will be used); (c) be in a position with a proven or anticipated need for Derivative Declassification Authority; and (d) be so designated in writing as described below.

      (2) Designation.

         (a) Requests for Derivative Declassification Authority for positions currently without such authority should be submitted in writing to DP-32. Such requests should include (1) the name and title of the individual for whom the authority is requested, (2) a description of the subject area and jurisdiction for which the authority is needed, (3) the anticipated frequency of use of the authority, (4) the qualifications of the individual for whom the authority is requested, and (5) any other information which would support the need for the authority.

         (b) When an individual vacates a position for which Derivative Declassification Authority has been granted, the name and

title of the individual losing the authority and the effective date of the loss of that authority must be sent by the individual's organization to DP-32.

(c) When an individual assumes a position for which Derivative Declassification Authority has already been granted, that individual's name, title, and qualifications must be submitted to DP-32 for approval. The individual may not assume the declassification authority of the position until his or her approval by DP-32.

(d) Derivative Declassification Authority may not be redelegated.

(3) Cancellation.

(a) If the Head of an organization determines that a position no longer requires Derivative Declassification Authority, DP-32 shall promptly be notified of the position title, the name of the person who holds or last held the position, and the effective date of cancellation of authority.

(b) If DP-32 or the Manager of the Operations Office determines that an individual no longer requires Derivative Declassification Authority, he or she shall advise the person concerned that such authority is to be cancelled, the date of cancellation, and the reasons for the cancellation.

(4) Recordkeeping Requirements. DP-32 shall maintain a list of all individuals with Derivative Declassification Authority. This list shall include (a) the name and title of the individual granted the authority, (b) the individual's Departmental Element or contractor organization, and (c) the effective date of the designation. In addition, each Departmental Element and contractor organization shall maintain a similar list of all individuals with Derivative Declassification Authority within its jurisdiction.

(5) Authority Definition. (See page X-23, Part C.)

(a) An individual with Derivative Declassification Authority may derivatively declassify or downgrade documents or material originated by his or her Departmental Element, its contractors, or the predecessors of these organizations. In certain circumstances, DP-32 may grant broader declassification authority to an individual.

(b) Derivative Declassifiers may declassify documents or material only in the areas in which they have been delegated such authority and which disclose only:

1 Information falling within the "unclassified" topics of classification and/or declassification guidance specifically authorized for their use in declassifying documents; or

2 Information identified as unclassified or that has been declassified by DP-32; or

3 Purely administrative information which reveals no technical or programmatic data. (Caution: This criterion is intended for historical documents and is to be interpreted very narrowly. If there is any doubt as to whether information is "purely administrative," specific guidance must be sought.)

PART B - AUTOMATIC DECLASSIFICATION AND DOWNGRADING

1. RESTRICTED DATA AND FORMERLY RESTRICTED DATA. Only DP-1 may declassify RD and FRD. DP-1 and DP-32 may downgrade RD and FRD. RD and FRD are not subject to automatic declassification or downgrading.

2. NATIONAL SECURITY INFORMATION. (See Chapter X, Part F, Figure X-3 for a summary conversion table on the duration of classification.)

   a. Documents Classified Pursuant to Executive Order 10290. Documents classified pursuant to Executive Order 10290 and marked for automatic downgrading or declassification should be downgraded and declassified in accordance with such markings.

   b. Documents Classified Pursuant to Executive Order 10501.

      (1) Groups 1 and 2. Documents under Groups 1 and 2 of Executive Order 10501, as amended by Executive Order 10964, are not automatically downgraded or declassified.

      (2) Group 3. Documents under Group 3 of Executive Order 10501, as amended by Executive Order 10964, shall be downgraded as follows: (a) Top Secret to Secret at 12 years from date of origin of the document; or (b) Secret to Confidential at 12 years from origin (unless the document was originally classified as Top Secret, in which case downgrade to Confidential at 12 years from the time it was downgraded to Secret).

      (3) Group 4. Documents under Group 4 of Executive Order 10501, as amended by Executive Order 10964, shall be downgraded as follows: (a) if originated on or before 12-1-66, they shall be declassified immediately; (b) if originated on or after 12-2-66 and on or before 5-31-72, they shall be downgraded to Confidential and declassified at 12 years from date of origin.

   c. Documents Classified Pursuant to Executive Order 11652.

      (1) Advanced Declassification Schedule. Documents marked for automatic downgrading in advance of the General Declassification Schedule (GDS) of Executive Order 11652 shall be downgraded in accordance with the schedule for downgrading marked on the documents. Unless otherwise specified on the documents, they will be subject to the GDS for the rest of the time they remain classified.

      (2) General Declassification Schedule. Documents marked as being subject to the GDS of Executive Order 11652 shall be downgraded as follows: (a) Top Secret to Secret at 2 years from date of origin of the document; (b) Secret to Confidential at 2 years from date of

origin (unless the document was originally classified as Top Secret, in which case it is 2 years from the time it was downgraded to Secret); and (c) Confidential documents will be declassified 6 years from date of origin (or from the date at which they were downgraded to Confidential).

(3) Documents Marked as Exempt From the General Declassification Schedule of Executive Order 11652 normally were not marked for automatic downgrading. When such documents have been marked for automatic downgrading, they shall be downgraded in accordance with the schedule for downgrading marked on the documents.

d. Documents Classified Pursuant to Executive Order 12065 and marked for automatic downgrading or declassification will be downgraded or declassified in accordance with such markings.

e. Documents Classified Pursuant to Executive Order 12356 and marked for automatic downgrading or declassification will be downgraded or declassified in accordance with such markings.

PART C - REVIEW OF DOCUMENTS FOR DECLASSIFICATION OR DOWNGRADING

1. GENERAL. Part C pertains to RD, FRD and NSI, except as noted on Page VI-10, paragraph 7. Previously generated classified documents shall be reviewed for possible declassification/downgrading in accordance with the procedures described below. Note that a determination that a document is unclassified does not mean that it can be released to the public. Other factors (e.g., FOIA exemptions such as section 148 of the Atomic Energy Act, Privacy Act exemptions, Patent Secrecy Act, or patent clearance review) may limit the releasability of all or part of the document.

   a. Documents as specified in (1) through (5) below may not be automatically declassified, but must be reviewed in accordance with procedures specified below as appropriate before they are declassified.

      (1) Documents with no markings which indicate declassification or review dates or events.

      (2) Documents marked as RD or FRD.

      (3) Documents assigned to Groups 1, 2, or 3 as defined in Executive Order 10964.

      (4) Documents Exempt from the General Declassification Schedule (XGDS) as defined in Executive Order 11652 and marked with a date or event for automatic declassification beyond 20 years from the date of origin of the documents (30 years for documents containing foreign government information), or for which the declassification period was impossible to determine or was indefinite at the time of origin.

      (5) Documents classified pursuant to Executive Order 12065 and assigned a date or event for review.

   b. Documents which carry conflicting declassification instructions will be handled in accordance with the most restrictive markings.

   c. Documents may be declassified only by Derivative Declassifiers and Original Classifiers under certain conditions prescribed in this manual. (See Chapter VI, Part A, and Chapter V, Part A, respectively.)

   d. In the declassification review process, referrals may be made, as appropriate, to Responsible Reviewers. It is also the responsibility of the Departmental Element or contractor organization initiating the review to obtain patent clearance where appropriate.

e. Under certain circumstances, DP-32 may determine that documents concerned with specific sensitive areas may be declassified only by certain declassifiers. Specific instructions will be issued when and if such occasions arise. If the reviewer decides that he or she is not sufficiently competent in the subject area addressed in the document to determine whether it may be declassified, or it is outside his or her jurisdiction, the matter must be referred to the local classification office, or, where appropriate, through channels to DP-32.

2. FORMAL REPORT REVIEW. This procedure is used for formal reports produced for or by DOE or its predecessors.

a. Formal reports are to be declassified only by a Derivative Declassifier in the local (i.e., DOE or contractor) classification office or DP-32. This authority may also be delegated to other specified Derivative Declassifiers.

b. When there is any doubt about whether a document should be declassified, it shall be referred through channels to DP-32 for resolution. Two copies of the formal report should be submitted along with a recommendation and evaluation to DP-32. A Classification Officer may also refer the report to an appropriate Responsible Reviewer.

c. Upon receipt of a request for a formal report review, DP-32 may transmit a copy of the report to an appropriate Responsible Reviewer. When Responsible Reviewers review reports under this provision, they shall transmit the copy of the report with their recommendations and evaluation to DP-32.

d. In its review, DP-32 will consider the comments of the Classification Officer submitting the request, the Responsible Reviewer, and any other organization asked to review the report prior to the final determination concerning declassification of the report. DP-32 will notify the Classification Officer who initiated the request, or the individual initiating the request when the request is made directly to DP-32, with regard to the final declassification determination.

e. If the report is to be declassified, upon receipt of notification of declassification from DP-32, the Classification Officer or other initiator of the declassification review shall assure that all holders of copies of the report are notified of the declassification.

3. REVIEW BY DERIVATIVE DECLASSIFIERS.

a. Derivative Declassifiers shall review documents or materials submitted to them for declassification review in accordance with the provisions of this Order. If, as a result of the review, documents or materials are to be determined declassifiable, the reviewer will declassify them. Documents or material determined not to be declassifiable under this authority, but possibly declassifiable under other authority, may be

referred by the Derivative Declassifiers for further processing to the Classification Officer or DP-32, as appropriate.

b. The person who declassifies a document shall assure that all known holders of its copies are promptly notified.

4. REVIEW BY ORIGINAL CLASSIFIERS. Authorized Original Classifiers may originally declassify NSI documents (other than formal reports) over which they have exclusive programmatic jurisdiction and which they, their predecessors, or subordinates, including contractor and/or subcontractor organizations under their cognizance, originally classified, provided the declassification is consistent with DOE policy. They may derivatively declassify RD, FRD, and NSI documents (other than formal reports) over which they have exclusive programmatic jurisdiction and which they, their predecessors, or subordinates, including contractor and/or subcontractor organizations under their cognizance, derivatively classified, provided the declassification is consistent with DOE policy and guidance. Derivative declassification actions must be based on the information appearing as an unclassified topic in a guide approved for the classifier's use in declassifying documents.

5. LARGE-SCALE REVIEWS (FILE CLEARANCE REVIEWS). Files containing classified documents that are obsolete or deal with an activity that has been declassified or discontinued may be reviewed to declassify those documents no longer requiring security protection. Reviews involving more than a small number of documents are subject to the following special requirements in addition to normal procedures:

a. Special reviews may be approved only by the cognizant DOE Classification Officer after coordination with DP-32. A request to conduct a special review at a contractor site must be submitted by the DOE contractor Classification Officer to the Operations Office. The Operations Office will review the proposal and may approve it only after written coordination with DP-32. (HQ and field elements should submit requests for such reviews at their sites to DP-32.)

b. All such requests shall include, at a minimum:

(1) A description of the nature of the review;

(2) An explanation of the requirement for the review;

(3) The identities and qualifications of the reviewers;

(4) A description of the classification guidance to be used on the review; and

(5) Detailed, written procedures for conducting the technical and clerical aspects of the review, including methods of quality assurance to be employed.

c. The review must be conducted under the direct supervision of the local classification officer (in Headquarters, DP-32).

d. As with all declassification reviews, extreme care must be exercised.

(1) Particular care must be taken to assure that sufficient time is allowed for a careful and thorough review of the documents.

(2) Reviewers must be rebriefed just prior to initiation of the review project to assure they are fully cognizant of their authorities and thoroughly understand the classification guidance to be used.

(3) Specific instructions must be given regarding treatment of information not covered explicitly in current classification guides.

6. PATENT APPLICATION REVIEW. GC-42 initiates requests for declassification review of all patent applications.

a. GC-42 shall transmit one copy of the patent application to DP-32 for review to determine if it may be declassified in accordance with current DOE classification policy.

b. DP-32 may refer questions about declassification of DOE patent applications to a Responsible Reviewer for review and recommendations. However, classified, private, non-DOE patent applications shall not be referred to a Responsible Reviewer without the express written approval of GC-42. Such special handling of patent applications as is necessary to comply with section 151(e) of the Atomic Energy Act and as may be required to protect the patent position of the U.S. Government will be observed.

c. Upon completion of the required review, DP-32 will return the patent application to GC-42 with the determination.

7. REVIEWS PURSUANT TO EXECUTIVE ORDER OR STATUTE. Executive Order 12356, the FOIA, and the Privacy Act contain provisions requiring classification review of information and documents. The procedures for carrying out such reviews are given in the following subparagraphs.

a. Executive Order 12356 requires the establishment of procedures for Mandatory Review for declassification of NSI. It also requires that systematic review guidelines be furnished to the Archivist of the United States for use in reviewing for declassification/downgrading of (1) classified documents accessioned into the National Archives of the United States, and (2) classified presidential documents under the Archivist's control which were originated by or contain information under the purview of DOE or its predecessors. Under Executive Order 12356, DP-32 may conduct internal and systematic review programs for classified information originated by DOE and contained in documents

determined by the Archivist to be permanently valuable, but which have not been accessioned into the National Archives of the United States.

(1) Mandatory Review for Declassification.

(a) Except as provided in section 3.4(b) of Executive Order 12356, all information classified by DOE under Executive Order 12356 or its predecessor orders (i.e., NSI) is subject to a review for declassification by DOE if the request:

1 Is made by a U.S. citizen or permanent resident alien, a Federal agency, or a State or local government;

2 Describes the document or material containing or revealing the NSI in question with sufficient specificity to enable it to be located with a reasonable effort; and

3 Is sent to the Director of Classification, U.S. Department of Energy, Washington, DC 20545.

(b) Invalid Requests. The requester will be notified promptly by DP-32 if his or her request is not valid. This notification letter will explain why the request cannot be processed and, if applicable, tell the requester what additional information is needed to allow processing of the request.

(c) Valid Requests. Upon receipt of a valid request for mandatory declassification review, DP-32 shall:

1 Contact all appropriate Departmental Elements requesting that their files be searched for documents and material responsive to the request.

2 On the basis of the results of the above search, determine whether estimated review and coordination time required to process the request precludes a prompt declassification determination and, if so, inform the requester of the additional time needed to process the request.

3 Review the documents or other material responsive to the request and determine whether or not the classified information under the purview of DOE contained in or revealed by the documents or other material can be declassified.

4 Coordinate with other agencies the review of documents or other material originated by DOE that are responsive to the request and that contain information under the purview of those agencies.

5 After deletion of all classified information under the purview of DOE, forward a copy of any documents or other material originated by another agency to that agency for further processing and direct response to the requester, including a copy of the request together with recommendations for action and, after consultation with the originating agency, inform the requester of the referral.

6 Transmit to the requester the final determination of DP-32 as to whether all or part of any documents or other material responsive to the request may be released to the requester. This determination must be made within 1 year from the date of receipt of the request except in unusual circumstances (e.g., delays caused by coordination of the review of responsive documents or other material originated by DOE with agencies having purview over information contained in or revealed by the documents or other material).

7 In those cases where a fee (see 10 CFR 1004.9 for schedule of fees charged for documents or material provided to requesters) is to be charged, notify the requester of the estimated amount of the fee and await confirmation by the requester of willingness to pay the fee.

8 In those cases where no fee is to be charged, or where the requester has agreed to pay the fee, and consistent with other applicable law, send the requester copies of declassified documents or other material or declassified portions of classified documents or other material that constitute coherent segments.

9 In those cases where all or part of documents or other material responsive to a request cannot be declassified, notify the requester that he or she has the right to an administrative appeal of the denial within 60 days of receipt of the denial letter. The requester shall be notified that the appeal shall specify why the requester believes the information in question does not warrant classification and, if possible, should include copies of the initial request letter and the denial letter from the Director of Classification. The appeal should be sent to the Assistant Secretary for Defense Programs, U.S. Department of Energy, Washington, DC 20545.

(d) Appeals of Denials of Mandatory Declassification Review Requests.

1 Immediately upon receipt of an appeal request, an ad hoc committee will be assembled and headed by a representative

from the Office of DP-1 and will be made up of representatives from any Departmental Element that he or she determines to have an interest in the appeal or in the information in question.

2 DP-32 will provide the committee all information, documents, and any other assistance pertinent to the appeal, and will advise the committee with regard to the classification of the information involved.

3 The committee will review the basis for the denial and transmit its findings and recommendations to DP-1 within 15 working days following receipt of the appeal.

4 On the basis of the committee report, DP-1 shall make a final determination on the appeal within 25 working days following receipt of the appeal. The head of the committee then shall notify the requester, within 30 working days following receipt of the appeal, in writing, of the final determination. In accordance with this determination and consistent with other applicable law, copies of declassified documents or other material or declassified portions of classified documents or other material responsive to the request will be released to the requester, upon payment of any required fees, and/or the requester will be given a statement as to why some or all of the documents or other material cannot be declassified.

(2) Systematic Review by the Archivist of the United States. Executive Order 12356 requires the Archivist of the United States to systematically review for declassification or downgrading (a) classified documents accessioned into the National Archives of the United States and (b) classified presidential documents under the Archivist's control. Such documents shall be reviewed in accordance with systematic review guidelines provided by DP-32 for information under the purview of DOE or its predecessors.

(a) Systematic Review Guidelines. DP-32 shall issue and maintain guidelines for systematic declassification review of information under the purview of DOE or its predecessors. These guidelines shall be developed in consultation with the Archivist and the Director of ISOO and designed to assist the Archivist in the conduct of systematic reviews. These guidelines shall be reviewed and updated at least every 5 years unless earlier review is requested by the Archivist.

(b) Assistance to the Archivist. DP-32 shall designate experienced personnel to provide timely assistance to the

Archivist in the systematic review process. Such personnel shall be designated as having Derivative Declassification Authority for the documents subject to the systematic review process that contain information under the purview of DOE or its predecessors.

(c) Internal Systematic Review Programs. DP-32 may conduct internal systematic review programs of documents containing information under the purview of DOE or its predecessors that have been determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States. DP-32 shall originate any required instructions or guidelines on a case-by-case basis for internal systematic review programs.

b. Freedom of Information Act or Privacy Act of 1974. Classification review and other actions regarding review of classified documents requested pursuant to the FOIA or the Privacy Act shall be conducted in accordance with the provisions of this Order and DOE orders concerning the FOIA and the Privacy Act.

c. Confirmation of Existence of Requested Documents. Individuals responding to requests for classified documents made pursuant to the FOIA, the Privacy Act, or the mandatory review provisions of Executive Order 12356 shall refuse to confirm or deny the existence or nonexistence of requested documents whenever the fact of their existence or nonexistence is itself classified.

8. OTHER REVIEWS BY THE OFFICE OF CLASSIFICATION.

a. Centralized Categorical Reviews. Under certain circumstances, DP-32 may determine that the declassification review of documents or material dealing with specified categories of information must be conducted by DP-32.

b. Priority Reviews. When the Head of a Departmental Element or his or her designated representative determines that an immediate declassification review is required of a document that is beyond the local declassification authority, he or she may request a priority review for declassification by DP-32. DP-32 will conduct the review as rapidly as possible and will return one copy of the document to the initiator of the declassification request with an official notification of final action. When the situation so warrants, a priority review should be explicitly requested, with a brief explanation as to the need for special handling. The purpose of the review and any special instructions should be included in the request.

9. DEPARTMENTAL AND CONTRACTOR REVIEW RESPONSIBILITY.

   a. Originating Departmental Element or Contractor Organization. That Departmental Element or contractor organization which originated a document must be consulted before declassification/downgrading of the document.

   b. Departmental Element or Contractor Organization With Programmatic Interest in a Document. Regardless of who originated it, any document containing information outside the programmatic jurisdiction of the declassifier must be coordinated with the Departmental Element(s) or contractor organization(s) having programmatic interest. In the case of other agency or foreign government information, see paragraph d, below. This coordination is particularly important when no single organization has sole programmatic jurisdiction over the information in a document.

   c. Director of Classification. DP-32 is authorized to make the final determination to declassify/downgrade documents originated by any Departmental Element or contractor organization. This authority may be delegated.

   d. External Coordination. DP-32 shall conduct all interagency or inter-Government coordination required to declassify/downgrade documents in the possession of DOE or its contractors. When DP-32 receives a request made pursuant to the FOIA, the Privacy Act, or the mandatory review provisions of Executive Order 12356 for classified documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, only after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response subject to the conditions specified on page VI-14, paragraph 7c of this part is required, DP-32 shall respond to the requester in accordance with that paragraph.

10. REPRODUCTION FOR DECLASSIFICATION REVIEW. Reproduction of documents for the sole purpose of facilitating their review for declassification shall not require the consent of the originator.

PART D - NOTIFICATION OF DECLASSIFICATION OR DOWNGRADING

1. GENERAL. Part D pertains to RD, FRD and NSI. Those authorizing a change in classification (declassification or downgrading) of documents will ensure that all holders of the documents are notified as follows.

   a. Top Secret Documents. The person authorizing the declassification or downgrading of a Top Secret document shall notify DP-34, who shall notify all custodians.

   b. Secret and Confidential Documents. The person authorizing the declassification or downgrading of a Secret or Confidential document shall ensure that all known holders of the document are notified.

   c. Documents Sent to the Office of Scientific and Technical Information. The person authorizing the declassification or downgrading of a document that has been sent to the Office of Scientific and Technical Information shall provide a copy of the change of classification notice to the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, Tennessee 37831, through the Director of Classification, for inclusion in the Office of Scientific and Technical Information data base.

   d. Forwarding of Notices. If the recipient of a declassification or downgrading notice has transmitted the document to another custodian, the change notice should be forwarded to the new custodian.

2. DECLASSIFICATION NOTICES.

   a. Declassification Notices shall be prepared, reviewed, and signed by the individual authorizing the declassification. It is the responsibility of this individual to ensure that the notice accurately and uniquely describes the document. In general, recipients of the notice (including the Office of Scientific and Technical Information) will not be in a position to verify its accuracy.

   b. Internal declassification notification may be handled by each Departmental Element and contractor organization according to its own requirements. Internal declassification notices shall contain, as a minimum, the following information:

      (1) Full title of the document. If the document is untitled, a description of the document sufficient to uniquely identify it shall be provided.

      (2) The identification number of the document (such as report number, short title, document number), if any.

      (3) The identity of the author, signer, or originator of the document.

(4) The document date.

(5) The number of pages in the document (from the documentation stamp on those documents with such a marking; otherwise, this is not required in the notice).

(6) The name of the Departmental Element or contractor organization that originated or issued the document.

(7) The original classification of the document.

(8) The identity of the person authorizing the declassification (by name, title, and organization).

(9) The effective date of the declassification action.

c. All declassification notices will also contain a statement worded substantially as follows:

> The custodian of the document described herein is authorized to remove, cancel, or otherwise void the classification markings from the document. Such markings may be removed only when the correspondence of this notice to the document has been verified by two persons, who must ensure that the document concerned identically fits the description provided herein. Otherwise, the markings may not be removed. If there is any doubt regarding the identity of the document to which this notice applies, the recipient should contact the originator of the notice for further information. The persons who remove the markings and validate that action shall mark the document as having been declassified, identify this notice as their authority for doing so, and sign and date the action on the document. If a person who receives this notice has given the document or copies thereof to others, this notice should also be forwarded to such other custodians.

d. Unless sanitization is specifically required or requested, reviewers will not sanitize documents. Moreover, notification of sanitization to other than the requester will not be issued. Each extract or deleted version of a numbered classified document (i.e., those with report numbers, document numbers, etc.) will be assigned a new, unique number. If necessary, the new version can also be identified as being an extract or deleted version of the original document. When an extract or deleted version is declassified, the declassification notice will specifically state that the document is an extract or deleted version, as appropriate.

PART E - RE-MARKING DECLASSIFIED OR DOWNGRADED DOCUMENTS

1. GENERAL. Part E pertains to RD, FRD and NSI, except as noted in paragraph 3, below.

2. REMOVAL OR CANCELLATION OF CLASSIFICATION MARKINGS FROM DOCUMENTS.

   a. Custodians of documents for which a written notification of declassification is received from an authorized source will ensure that the document concerned exactly corresponds to the description given in the declassification notice before removing or cancelling the classification markings. Custodians of formal reports may declassify them only on the basis of formal declassification notices issued by the Office of Scientific and Technical Information. However, custodians in the same organization in which a declassification determination of a formal report has been made may act upon notification from the appropriate declassification authority in accordance with local procedures without having to wait for formal notification from the Office of Scientific and Technical Information. Custodians of documents other than formal reports may declassify them only on the basis of a written declassification notice from an authorized source. At least two persons must verify the applicability of the declassification notice to the document concerned.

   b. If there is any doubt regarding the identity of a document to be declassified, the document should not be declassified. If there is any doubt regarding the identification of a document for which a declassification notice has been received, the custodian shall contact the person authorizing the declassification for more specific identification or confirmation. If clarification is needed for declassification notices published by the Office of Scientific and Technical Information for formal reports, the custodian should contact DP-32 for identification of the person authorizing declassification.

   c. When the classification markings are removed or cancelled from a document pursuant to a declassification notice or shall be marked to show:

      (1) The signature of the person removing the markings and the date of the action;

      (2) The signature of the person verifying the validity of the action and the date of verification; and

      (3) The authority for declassifying the document (e.g., a memorandum, an Office of Scientific and Technical Information notice, a classification guide, or guide topic).

Classification changed to Unclassified
(Insert appropriate classification)

by authority of Bulletin ABC 4/4/82
(Authority for change in classification) (Date)

by G. H. Iverson 5/5/83 J. K. Lawson 6/6/84
(Signatures of persons making change and verifying the information) (Date)

Figure VI-1
Example of Document Declassification/Downgrading Marking

3. AUTOMATIC DECLASSIFICATION. An NSI document marked with a date or event for automatic declassification may be declassified by any custodian of the document when that date or event has occurred. The declassification/downgrading marking illustrated in Figure VI-1, above, is not required.

CHAPTER VII
EDUCATION

1. OBJECTIVE. Employees of DOE, its contractors, and others who generate or have access to classified information must have sufficient understanding of classification policies, principles, and procedures to discharge their duties. The classification education program is intended to provide such an understanding.

2. EDUCATION PROGRAMS.

   a. Initial Classification Education. All new DOE and DOE contractor employees must understand their classification responsibilities before being given access to classified information. Therefore, in preparation, they shall be given a classification orientation which shall, as a minimum:

      (1) Explain what classification and classified information are, including the classification levels and the difference between RD, FRD, and NSI.

      (2) Explain the local classification organizational structure and the channels through which new employees should refer classification questions.

      (3) Stress the individual's responsibility for assuring that documents are reviewed for classification. In addition, employees who require knowledge of classification guidance in their work should have such guidance explained to them. This may be accomplished either during the initial orientation or at some reasonable time thereafter.

   b. Continuing Education. All DOE and DOE contractor classification offices shall conduct a continuing classification education program to maintain classification awareness and apprise employees of changes in classification policies and procedures.

   c. Classifier/Declassifier Briefing. Before an individual becomes an Original or Derivative Classifier or Derivative Declassifier, a local classification representative shall explain in detail the classification guidance pertaining to the classifier's subject area, and the special procedures which may apply. Periodic updates shall be given every 2 years or as changes in classification policy or procedures occur.

   d. Special Briefings. Periodically, a classification representative shall conduct special oral or written briefings. Such briefings may be required, for example, because of the issuance of new guidance in a particular subject area or because of a change in classification procedures,

such as redefinition of the authority of a Secret Original Classifier. Such briefings might be conducted, for example, for all individuals in a given Departmental Element or contractor organization who are involved in the affected technical area or who have the redefined classification authority. The need for such briefings may be identified by the local classification office or by the potential attendees.

3. OTHER CLASSIFICATION EDUCATION METHODS. Classification Officers are encouraged to provide continuity to their classification education program by utilizing some or all of the following suggested methods:

   a. Impress supervisors with the importance of observing classification guidance and procedures, and urge them to do likewise for their subordinates.

   b. Encourage discussions of specific classification items and problems at staff meetings.

   c. Invite outside speakers in the classification field to address employees on specific aspects of the classification and declassification programs.

   d. Invite technical and scientific personnel to speak in areas in which they have particular expertise and where classification determinations may have an impact.

   e. Use internal publications, posters, and so forth, for classification messages.

   f. Share information concerning classification efforts with other DOE and DOE contractor classification offices.

4. PRIVATE ORGANIZATIONS AND INDIVIDUALS. The statutory definition of RD is not limited to data developed in government programs but includes all data that meet the statutory definition of RD, including data generated in private work.

   a. DOE is responsible under the Atomic Energy Act for monitoring R&D conducted by private organizations and individuals.

   b. DP-32 is responsible for educating private organizations and individuals insofar as classification concerns affect their activities. Such education will be carried out primarily by publication of relevant information in the "Federal Register."

   c. Field classification personnel will assist in this portion of the education program by advising DP-32 of private R&D or other activity likely to generate RD and where, consequently, there is a need for classification education.

CHAPTER VIII

CLASSIFICATION APPRAISALS

1. POLICY. The classification practices, procedures, and performance of DOE and DOE contractor organizations shall be appraised to ascertain their adequacy and effectiveness.

2. OBJECTIVES.

   a. To determine the effectiveness of classification personnel in implementing the classification program.

   b. To determine whether classification practices and performance conform to DOE policy.

   c. To evaluate the effectiveness of locally developed methods of implementing DOE classification policy and regulations.

   d. To evaluate the adequacy of the classification guidance and control provided by DOE and DOE contractor organizations to those within their supervision.

3. STANDARDS AND PROCEDURES.

   a. Appraisal Guidance and Instructions. This chapter presents policy, objectives, and general guidance regarding standards and procedures to be used in conducting classification appraisals. Detailed instructions and specific guidance on the conduct of appraisals, including preparation for appraisals, suggested formats for workpapers and reports, and suggested methods for gathering and evaluating relevant information, are contained in the classification appraisal procedural guide developed and promulgated under the authority of DP-32.

   b. Scope of Appraisals. The classification programs of the various Departmental Elements and DOE contractor organizations differ in scope, complexity and sensitivity. No single list of points to be covered in an appraisal is, therefore, appropriate in all cases. The list of areas below is presented merely as a guideline; it should serve to introduce a measure of uniformity into appraisal reports and to remind the appraisers of areas that may need attention. An appraisal should provide answers to those of the following questions that are applicable:

      (1) Management Awareness. How actively does management keep informed of current DOE classification policy, especially as it applies to information, projects, and materials under their purview?

      (2) Management Support. What is the position of the classification function and the Classification Officer in the organization? Are sufficient resources available to the Classification Officer? If the Classification Officer has additional duties, do the

Classification Officer and any assistants devote sufficient time to classification matters?

(3) Practices. How closely do classification practices comport with DOE policy? (The answer should be based on a review of representative samplings of classified and unclassified correspondence, records, procurement forms, financial reports, etc.).

(4) Classification Guidance. How complete, effective, and timely is the guidance developed for classified projects? (Appraisal of a prime contractor organization should include review of the classification guidance of both the prime and subcontractor organizations and the resulting classification practices.) Have local classification guides been prepared for all classified work being performed? Are they kept current?

(5) Education Program. How active and effective is the education program for indoctrination and instruction of all individuals in classification policies and procedures?

(6) Classification Board. If a board has been appointed, what is its purpose, who is on it, what is the frequency of its meetings, and is it effective?

(7) Classifying and Declassifying Officials. How current is the appointment of Authorized Classifiers and Authorized Declassifiers? Are their numbers, locations, and qualifications appropriate?

(8) Declassification. Is a declassification program needed? If there is a program, is it being effectively administered?

(9) Appraisals. How thorough is the appraisal system in determining compliance with approved guidance? Are subcontractor appraisals being conducted?

(10) Other Classifying Organizations. Do any organizations other than DOE (for example, DOD) have classification responsibilities regarding sole or joint programs at the organization being appraised? If there are inconsistencies between DOE classification guidance and other guidance, have actions been taken to resolve them?

(11) Nonnuclear Programs. In field elements with jurisdiction over nonnuclear programs, have procedures been implemented for periodic review of these programs for possible need for classification? If so, are these review procedures timely and comprehensive? Have the personnel responsible for the review been properly trained and designated with appropriate classification authority?

c. Frequency of Appraisals. The scope and frequency of appraisals shall be determined by the management of the appraising Departmental Element after consideration of the following factors:

(1) Past Performance Experience and Appraisal Results. Problem areas and key functions representing potential trouble spots should be identified for frequent review.

(2) Interval Since Last Appraisal. Every function having a major classification interest should be appraised at least every 3 years unless particular circumstances indicate otherwise. Functions having a minor classification interest may be appraised on a 5-year or longer basis.

(3) Management's need for information.

(4) Number of classified contracts administered by a Departmental Element.

d. Visits.

(1) Classification performance should be evaluated on the basis of a visit to the Departmental Element or contractor organization being appraised. A classification appraisal based not on a visit but on performance as revealed by matters raised by the organization itself or incidentally exposed may neglect many factors. Various units within the Departmental Element or contractor organization may be unaware that their classification practices are incorrect or may be reluctant to call attention to them. Appraisals of a Departmental Element or contractor organization based on personal visits should include an inspection of classification practices of the various units and a classification review of both outgoing and internal papers and records. In cases where visits for classification appraisals may be impractical (e.g., that of a contractor who has responsibility for numerous small subcontractors), appraisals may be made without visits, provided all other requirements of this Order regarding appraisals are met.

(2) Written records should be kept of all information gathered during a classification appraisal. These records form the basis for the conclusions presented in the appraisal report and can serve to clarify or substantiate these conclusions. A suggested format for these written appraisal records is given in the classification appraisal procedural guide.

e. Appraisal Reports.

(1) A written appraisal report is required. It should include sufficient evaluation of the scope of the classification program

listed on page VIII-1, paragraph 3, or equivalent treatment at the discretion of the appraiser, to give a clear picture of classification performance.

(2) A format for appraisal reports is given in the classification appraisal procedural guide. Use of this format is recommended in order to increase the comparability and uniformity of appraisals.

(3) The report should inform both the Departmental Element appraised and the organization responsible for the appraisal of the adequacy of the classification program, and list as recommendations any problem areas and necessary corrective actions. If a substantial number of recommendations appear in the report, they should be summarized for ready reference.

(4) Generally, no final report should be made without first informing the Head of the appraised Departmental Element of the appraisal results and the probable content of the report.

(5) The appraisal report on a Departmental Element shall be submitted to the Head of that Departmental Element, and copies forwarded to the HQ element with primary interest in its operations, DP-1, and, if appropriate, to other Secretarial officers.

(6) The appraisal report on an area element or a contractor organization by the field element administering the contract shall be filed in that field element, and a copy provided on request to DP-32.

(7) The appraisal report on a subcontractor organization by the contractor organization administering the contract shall be on file at the contractor organization, and a copy provided to the Departmental Element administering the prime contract.

f. Followup.

(1) Where recommendations for action on minor deficiencies have been submitted to responsible management, the adequacy of their implementation shall normally be determined and reported in the next appraisal. However, if measures are required to correct major deficiencies, a followup, at least by correspondence, shall be instituted by the appraising Departmental Element or contractor organization in a timely manner.

(2) A schedule for implementation of any necessary corrective actions should be prepared by the appraised Departmental Element or contractor organization and submitted to the appraising Departmental Element or contractor organization, which should institute measures to monitor the progress of implementation of corrective measures.

CHAPTER IX

CLASSIFICATION VIOLATIONS

1. VIOLATIONS SUBJECT TO SANCTIONS. DOE and DOE contractor personnel shall be subject to appropriate sanctions if they:

   a. Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under the Atomic Energy Act of 1954, as amended, Executive Order 12356, or predecessor Executive Orders;

   b. Knowingly, willfully, or negligently classify or continue the classification of information, documents, or materials in violation of Executive Order 12356, its implementing directives, this Order, or approved classification guidance;

   c. Knowingly and willfully violate any other classification provisions of Executive Order 12356, its implementing directives, or this Order; or

   d. Knowingly and willfully violate any provision of the Atomic Energy Act with regard to the classification or declassification of information under the purview of that Act.

2. REPORTING VIOLATIONS. When such violations occur, Heads of Departmental Elements shall promptly notify DP-32 and DP-34 through appropriate channels. Violations under paragraphs 1(a) and 1(b) above involving NSI will be promptly reported to ISOO by DP-34.

3. CORRECTIVE ACTIONS. Sanctions for such violations may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law. Heads of Departmental Elements wherein such violations occur shall ensure that appropriate and prompt corrective action is taken (including action to prevent recurrence).

CHAPTER X

REFERENCES AND OPERATING PROCEDURES

PART A - ATOMIC ENERGY ACT EXCERPTS

1. GENERAL. Pursuant to the Department of Energy Organization Act and the Energy Reorganization Act of 1974, as amended, the Secretary of Energy has certain responsibilities with regard to the control of information which falls under the purview of the Atomic Energy Act. In accordance with the Atomic Energy Act, it is DOE policy to control the dissemination and declassification of RD in such a manner as to assure the common defense and security. All information falling within the definition of RD is classified at its inception by the Atomic Energy Act.

2. DECLASSIFICATION AND TRANSCLASSIFICATION are also provided for by the Act. The five provisions of the Atomic Energy Act excerpted below deal with declassification or transclassification (section 142, Atomic Energy Act):

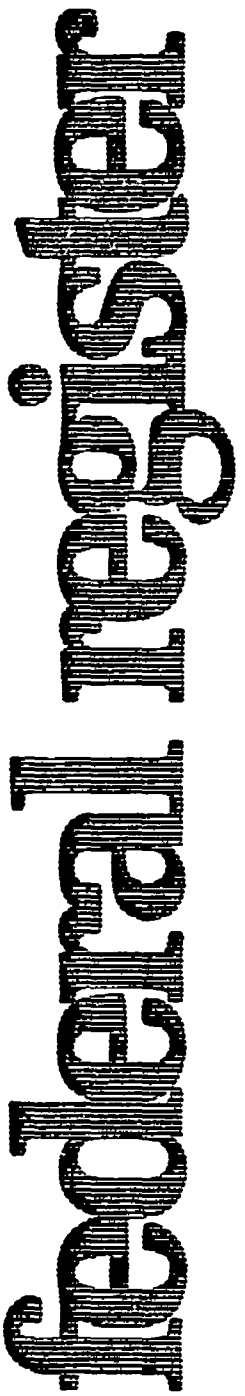
> "a. The [Secretary of Energy] shall from time to time determine the data, within the definition of Restricted Data, which can be published without undue risk to the common defense and security and shall thereupon cause such data to be declassified and removed from the category of Restricted Data.
>
> "b. The [Secretary of Energy] shall maintain a continuous review of Restricted Data and of any classification guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data which have been declassified in order to determine which information may be declassified and removed from the category of Restricted Data without undue risk to the common defense and security.
>
> "c. In the case of Restricted Data which the [Secretary of Energy] and the Department of Defense jointly determine to relate primarily to the military utilization of atomic weapons, the determination that such data may be published without constituting an unreasonable risk to the common defense and security shall be made by the [Secretary of Energy] and the Department of Defense jointly, and if the [Secretary of Energy] and the Department of Defense do not agree, the determination shall be made by the President. [Provision for declassification of FRD.]

"d. The [Secretary of Energy] shall remove from the Restricted Data category such data as the [Secretary of Energy] and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the [Secretary of Energy] and the Department of Defense jointly determine can be adequately safeguarded as defense information: provided, however, that no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with subsection 144b [of the Atomic Energy Act]. [Provision for the transclassification of RD to FRD.]

"e. The [Secretary of Energy] shall remove from the Restricted Data category such information concerning the atomic energy programs of other nations as the [Secretary of Energy] and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 102(d) of the National Security Act of 1947, as amended, and can be adequately safeguarded as defense information."

PART B - EXECUTIVE ORDER 12356 AND DIRECTIVE NO. 1

1. EXECUTIVE ORDER 12356:



Tuesday
April 6, 1982

Part IV

The President

Executive Order 12356—National Security Information

14874

Federal Register
Vol. 47, No. 66
Tuesday, April 6, 1982

Presidential Documents

Title 3—
The President

Executive Order 12356 of April 2, 1982

National Security Information

TABLE OF CONTENTS

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 *Classification Levels.*

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 *Classification Authority.*

(a) *Top Secret.* The authority to classify information originally as Top Secret may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; and

(3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret.* The authority to classify information originally as Secret may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential.* The authority to classify information originally as Confidential may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret or Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(d) *Delegation of Original Classification Authority.*

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification author-

ity; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.3 *Classification Categories.*

(a) Information shall be considered for classification if it concerns:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) foreign government information;

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States;

(6) scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Sec. 1.4 *Duration of Classification.*

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 *Identification and Markings.*

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) one of the three classification levels defined in Section 1.1;

(2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) the agency and office of origin; and

(4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 *Limitations on Classification.*

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

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

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information

may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 *Use of Derivative Classification.*

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1); and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 *Declassification Authority.*

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

Sec. 3.2 *Transferred Information.*

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 *Systematic Review for Declassification.*

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.4. *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 *General Restrictions on Access.*

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 *Special Access Programs.*

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

Sec. 4.3 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 *Policy Direction.*

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 *Information Security Oversight Office.*

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 *General Responsibilities.*

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official

designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

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

(d) Each agency head or the senior official designated under Section 5.3(a)(1) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 *Definitions.*

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) 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.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 *General.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and

declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

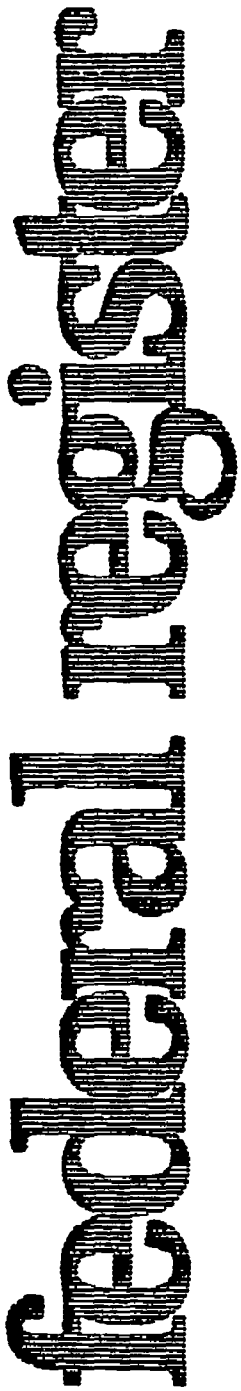
Ronald Reagan

THE WHITE HOUSE,
April 2, 1982.

[FR Doc. 82-9320
Filed 4-2-82; 2:52 pm]
Billing code 3195-01-M

Editorial Note: The President's statement of Apr. 2, 1982, on signing Executive Order 12356 is printed in the *Weekly Compilation of Presidential Documents* (vol. 18, no. 13)

2. 32 CFR PART 2001 (DIRECTIVE NO. 1)



Friday
June 25, 1982

Part VIII

Information Security Oversight Office

National Security Information

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

[Directive No. 1]

National Security Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Implementing Directive; final rule.

SUMMARY: The Information Security Oversight Office is publishing this Directive (final rule) pursuant to section 5.2(b)(1) of Executive Order 12356, relating to national security information. The National Security Council approved this Directive on June 22, 1982. The Executive order prescribes a uniform information security system; it also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of national security information.

EFFECTIVE DATE: August 1, 1982.

FOR FURTHER INFORMATION CONTACT:
Steven Garfinkel, Director, ISOO. Telephone: 202-535-7251.

SUPPLEMENTARY INFORMATION: This Directive is issued pursuant to the provisions of section 5.2(b)(1) of Executive Order 12356. The purpose of the Directive is to assist in implementing the Order; users of the Directive shall refer concurrently to that Order for guidance.

List of Subjects in 32 CFR Part 2001

Archives and records, Authority delegations, Classified information, Executive orders, Freedom of information, Information, Intelligence, National defense, National security information, Presidential documents, Security information, Security measures.

Title 32 of the Code of Federal Regulations, Part 2001, is revised to read as follows:

PART 2001—NATIONAL SECURITY INFORMATION

Authority: Section 5.2(b)(1), E.O. 12356, 47 FR 14874, April 6, 1982.

Subpart A—Original Classification

§ 2001.1 Classification levels.

(a) *Limitations [1.1(b)].*[1] Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only" or "Limited Official Use," shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify nonclassified executive branch information.

(b) *Reasonable doubt [1.1(c)].* (1) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" information in accordance with Subpart D, pending the determination about its classification. Upon the determination of a need for classification, the information that is classified shall be marked as provided in § 2001.5.

(2) When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level in accordance with Subpart D, pending the determination about its classification level. Upon the determination of its classification level, the information shall be marked as provided in § 2001.5.

[1] Bracketed references pertain to related sections of Executive Order 12356.

§ 2001.2 Classification authority.

(a) *Requests for original classification authority [1.2 and 5.2(b)(5)].* A request for original classification authority pursuant to section 1.2 of Executive Order 12356 (hereinafter "the Order") shall include a complete justification for the level of classification authority sought, a description of the information that will require original classification, and the anticipated frequency of original classification actions.

(b) *Listing classification authorities [1.2].* Agencies shall maintain a current listing of officials delegated original classification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

(c) *Exceptional cases [1.2(e)].* Information described in section 1.2(e) of the Order shall be protected as provided in § 2001.1(b).

§ 2001.3 Classification categories.

(a) *Classification in context of related information [1.3(b)].* Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(b) *Unofficial publication or disclosure [1.3(d)].* Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Order or predecessor orders, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences.

§ 2001.4 Duration of classification.

(a) *Information not marked for declassification [1.4].* Information classified under predecessor orders that is not subject to automatic declassification shall remain classified until reviewed for declassification.

(b) *Authority to extend automatic declassification determinations [1.4(b)].* The authority to extend the

classification of information subject to automatic declassification under predecessor orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

§ 2001.5 Identification and markings (1.5(a), 1.5(b) and 1.5(c)).

A uniform information security system requires that standard markings be applied to national security information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents created after the effective date of the Order shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper documents, or the originator shall provide holders or recipients of the information with written instructions for protecting the information.

(a) *Classification level.* The markings "Top Secret," "Secret," and "Confidential" are used to indicate: that information requires protection as national security information under the Order; the highest level of classification contained in a document; and the classification level of each page and, in abbreviated form, each portion of a document.

(1) *Overall marking.* The highest level of classification of information in a document shall be marked in such a way as to distinguish it clearly from the informational text. These markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) *Page marking.* Each interior page of a classified document shall be marked at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

(3) *Portion marking.* Agency heads may waive the portion marking requirement for specified classes of documents or information only upon a written determination that: (i) There will be minimal circulation of the specified documents or information and minimal potential usage of these documents or information as a source for derivative classification determinations; or (ii) there is some other basis to conclude that the potential benefits of portion marking are clearly outweighed by the increased administrative burdens. Unless the portion marking requirement has been waived as authorized, each portion of a document, including subjects and titles, shall be marked by placing a parenthetical designation immediately preceding or following the text to which it applies. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. If the application of parenthetical designations is not practicable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification, and the information that is not classified. If all portions of a document are classified at the same level, this fact may be indicated by a statement to that effect. If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(b) *Classification authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as follows:

"CLASSIFIED BY (identification of original classification authority)"

(c) *Agency and office of origin.* If the identity of the originating agency and office is not apparent on the face of a document, it shall be placed below the "CLASSIFIED BY" line.

(d) *Declassification and downgrading instructions.* Declassification and, as applicable, downgrading instructions shall be shown as follows:

(1) For information to be declassified automatically on a specific date:

"DECLASSIFY ON: (date)"

(2) For information to be declassified automatically upon occurrence of a specific event:

"DECLASSIFY ON: (description of event)"

(3) For information not to be declassified automatically:

"DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED or 'OADR' "

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

"DOWNGRADE TO (classification level) ON (date or description of event)"

(e) *Special markings.*—(1) *Transmittal documents [1.5(c)].* A transmittal document shall indicate on its face the highest classification of any information transmitted by it. It shall also include the following or similar instruction:

(i) For an unclassified transmittal document:

"UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED"

(ii) For a classified transmittal document:

"UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal document standing alone)"

(2) *"Restricted Data" and "Formerly Restricted Data" [6.2(a)].* "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence sources or methods [1.5(c)].* Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by the Director of Central Intelligence:

"WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED"

(4) *Foreign government information [1.5(c)].* Documents that contain foreign government information shall include either the marking "FOREIGN GOVERNMENT INFORMATION," or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(5) *Computer output [1.5(c)].* Documents that are generated as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(6) *Agency prescribed markings [1.5(c), 4.2(a), and 5.3(c)].* Officials delegated original classification authority by the President may prescribe additional markings to control reproduction and dissemination, including markings required for special access programs authorized by section 4.2(a) of the Order.

(f) *Electrically transmitted information (messages) [1.5(c)].* National security information that is transmitted electrically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A "CLASSIFIED BY" line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date:

"DECL: (date)"

(ii) For information to be declassified upon occurrence of a specific event:

"DECL: (description of event)"

(iii) For information not to be automatically declassified which requires the originating agency's determination (see also § 2001.5(d)(3)):

"DECL: OADR"

(iv) For information to be automatically downgraded:

"DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur)"

(4) Portion marking shall be as prescribed in § 2001.5(a)(3);

(5) Special markings as prescribed in § 2001.5(e) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended;

(ii) Information concerning intelligence sources or methods: "WNINTEL," unless prescribed by the Director of Central Intelligence;

(iii) Foreign government information: "FGI," or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the message shall be marked as if it were wholly of U.S. origin.

(6) Paper copies of electrically transmitted messages shall be marked as provided in § 2001.5(a) (1) and (2).

(g) *Changes in classification markings [1.4(b) and 4.1(b)].* When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

§ 2001.6 Limitations on classification [1.6(c)].

Before reclassifying information as provided in section 1.6(c) of the Order, the authorized official shall consider the following factors, which shall be addressed in the report to the Director of the Information Security Oversight Office:

(a) The elapsed time following disclosure;

(b) The nature and extent of disclosure;

(c) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed;

(d) The ability to prevent further disclosure; and

(e) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Subpart B—Derivative Classification

§ 2001.20 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

§ 2001.21 Classification guides.

(a) *General [2.2(a)].* Classification guides shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which classification level applies to each element or category of information; and

(3) Prescribe declassification instructions for each element or category of information in terms of (i) a period of time, (ii) the occurrence of an event, or (iii) a notation that the information shall not be declassified automatically without the approval of the originating agency.

(b) *Requirement for review [2.2(a)].* Classification guides shall be reviewed at least every two years and updated as necessary. Each agency shall maintain a list of its classification guides in current use.

(c) *Waivers [2.2(c)].* An authorized official's decision to waive the requirement to issue classification guides for specific classes of documents or information should be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

§ 2001.22 Derivative identification and markings [1.5(c) and 2.1(b)].

Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.5(a) through (e) as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(a) *Classification authority.* The authority for classification shall be shown as follows:

"CLASSIFIED BY (description of source document or classification guide)"

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown as follows:

"CLASSIFIED BY MULTIPLE SOURCES"

In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

(b) *Declassification and downgrading instructions.* Dates or events for automatic declassification or downgrading, or the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a "DECLASSIFY ON" line as follows:

"DECLASSIFY ON: (date; description of event; or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))"

Subpart C—Declassification and Downgrading

§ 2001.30 Listing declassification and downgrading authorities [3.1(b)].

Agencies shall maintain a current listing of officials delegated declassification or downgrading authority by name, position, or other identifier. If possible, this listing shall be unclassified.

§ 2001.31 Systematic review for declassification [3.3].

(a) *Permanent records.* Systematic review is applicable only to those classified records and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-permanent records.* Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) *Responsibilities.* (1) In meeting responsibilities assigned by section 3.3(a) of the Order, the Archivist shall:

(i) Establish procedures, in consultation with the Director of the Information Security Oversight Office, for the systematic declassification review of permanent classified records accessioned into the National Archives and classified presidential papers or records under the Archivist's control;

(ii) Conduct systematic declassification reviews in accordance with guidelines provided by the head of the agency that originated the information; or, with respect to foreign government information, in accordance with guidelines provided by the head of the agency having declassification jurisdiction over the information, or, if no guidelines have been provided, in accordance with the general guidelines provided by the Director of the Information Security Oversight Office after coordination with the agencies having declassification authority over the information; or, with respect to presidential papers or records, in accordance with guidelines developed by the Archivist and approved by the National Security Council;

(iii) Conduct systematic declassification reviews of accessioned records and presidential papers or records as they become 30 years old, except for file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and information concerning cryptology created after 1945;

(iv) Conduct systematic declassification reviews of accessioned records and presidential papers or records in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945 and cryptology records created after 1945 as they become fifty years old;

(v) Establish systematic review priorities for accessioned records and presidential papers or records based on the degree of researcher interest and the potential for declassifying a significant portion of the information;

(vi) Re-review for declassification accessioned records and presidential papers or records upon the determination that the followup review will be productive, both in terms of researcher interest and the potential for declassifying a significant portion of the information.

(2) The Archivist may review for declassification, with the concurrence of the originating agency, accessioned records and presidential papers or records, prior to the timeframes established in paragraphs (c)(1) (iii) and (iv) of this section.

(3) Officials delegated original classification authority by the President under the Order or predecessor orders shall:

(i) Within six months of the effective date of the Order issue guidelines for systematic declassification review and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designed to assist the Archivist in the conduct of systematic reviews;

(ii) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;

(iii) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(4) Within six months of the effective date of the Order the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist and the agencies having declassification authority over the information, general guidelines for the systematic declassification review of foreign government information. Also within six months, agency heads may issue, in consultation with the Archivist and the Director of the Information Security Oversight Office, specific systematic declassification review guidelines for foreign government information over which the agency head has declassification authority. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(d) *Special procedures.* All agency heads shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities), or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

§ 2001.32 Mandatory review for declassification [3.4].

(a) *U.S. originated information.* (1) Each agency head shall publish in the Federal Register the identity of the person(s) or office(s) to which mandatory declassification review requests may be addressed.

(2) *Processing.* (i) *Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Agency responses to mandatory declassification review requests shall be governed by the amount of search and review time required to process the request. In responding to mandatory declassification review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. Agencies shall make a final determination within one year from the date of receipt except in unusual circumstances. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its

possession that were originated by another agency, it shall forward the request to that agency. The forwarding agency shall include a copy of the records requested together with its recommendations for action. Upon receipt, the originating agency shall process the request in accordance with § 2001.32(a)(2)(i). Upon request, the originating agency shall communicate its declassification determination to the referring agency.

(iii) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 30 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(b) *Foreign government information.* Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2001.32(a). The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If the agency receiving the request is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(c) *Cryptologic and intelligence information.* Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(d) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 483a of title 31, United States Code. The schedules of fees published in the Federal Register by agencies in implementation of Executive Order 12065 shall remain in effect until they are revised.

§ 2001.33 Assistance to the Department of State [3.3(b)].

Heads of agencies should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

§ 2001.34 FOIA and Privacy Act requests [3.4].

Agency heads shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification. For information in special access programs established under the provisions of section 4.2 of the Order, the safeguarding requirements of Subpart D may be modified by the agency head responsible for creating the special access program as long as the modified requirements provide appropriate protection for the information.

§ 2001.41 Standards for security equipment [4.1(b) and 6.1(b)].

The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2001.42 Accountability [4.1(b)].

(a) *Top Secret.* Top Secret control officials shall be designated to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually. Agency heads may waive the requirement for an annual inventory of storage systems containing large volumes of Top Secret information upon a determination that the safeguarding of this information is not jeopardized by the inventory waiver. Waivers shall be in writing and be available for review by the Information Security Oversight Office.

(b) *Secret and Confidential.* Agency heads shall prescribe accountability or control requirements for Secret and Confidential information.

§ 2001.43 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum requirements for physical barriers.* (1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2001.41. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position changeable combination padlock. Heads of agencies shall prescribe supplementary controls for storage of Secret information in cabinets equipped with a steel lock bar. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, closed areas or similar facilities shall be controlled in accordance with requirements established by the appropriate agency head. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(b) *Combinations.* (1) *Equipment in service.* Combinations to dial-type locks shall be changed only by persons having an appropriate security clearance, and shall be changed whenever such equipment is placed in use; whenever a person knowing the combination no

longer requires access to it; whenever a combination has been subjected to possible compromise; whenever the equipment is taken out of service; or at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information that is protected by the lock.

(2) *Equipment out of service.* When security equipment is taken out of service it shall be inspected to ensure that no classified information remains, and the built-in combination lock shall be reset to the standard combination 50–25–50. Combination padlocks shall be reset to the standard combination 10–20–30.

(c) *Keys.* Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

§ 2001.44 Transmittal [4.1(b)].

(a) *Preparation and receipting.* Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads if conditions provide at least equivalent protection to prevent access by unauthorized persons.

(b) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for the purpose, or over authorized secure communications circuits.

(c) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) *The 50 States, the District of Columbia, and Puerto Rico.* Secret information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information, by the U.S. Postal Service registered mail, or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned.

(2) *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2001.44(c)(1) by one of the means established for Top Secret information, or by U.S. registered mail through Military Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

(d) *Transmittal of Confidential.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by the U.S. Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

(e) *Hand carrying of classified information.* Agency regulations shall prescribe procedures and appropriate restrictions concerning the escort or hand carrying of classified information, including the hand carrying of classified information on commercial carriers.

§ 2001.45 Special access programs [1.2(a) and 4.2(a)].

Agency heads designated pursuant to section 1.2(a) of the Order may create or continue a special access program if:

(a) Normal management and safeguarding procedures do not limit access sufficiently; and

(b) the number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2001.46 Reproduction controls [4.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electrically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret and Confidential documents may be reproduced to the extent required by operational needs.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

§ 2001.47 Loss or possible compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The agency under whose cognizance the loss or possible compromise occurred shall initiate an inquiry to (a) determine cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary, or legal action.

§ 2001.48 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, United States Code, which govern disposition of Federal records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude recognition or reconstruction of the classified information or material.

§ 2001.49 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for: (a) Protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct supervision of

authorized persons; and (b) meeting accountability requirements prescribed by the head of the agency.

§ 2001.50 Emergency planning [4.1(b)].

Agencies shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2001.51 Emergency authority [4.1(b)].

Those officials delegated original classification authority by the President may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

Subpart E—Implementation and Review

§ 2001.60 Agency regulations [5.3(b)].

Each head of an agency shall issue regulations in accordance with 5 U.S.C. 552(a) to implement the Order and 32 CFR Part 2001 no later than December 31, 1982. Those portions that affect members of the public shall include, at a minimum, information relating to the agency's mandatory declassification review program and instructions for submitting suggestions or complaints regarding the agency's information security program.

§ 2001.61 Security education [5.3(a)].

Each agency that creates or handles national security information is required under the Order to establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

§ 2001.62 Oversight [5.3(a)].

Agency heads shall require that periodic formal reviews be made to ensure compliance with the provisions of the Order and ISOO directives.

Subpart F—General Provisions

§ 2001.70 Definitions [6.1].

(a) *Original classification authority.* The authority vested in an executive branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(b) *Classification guide.* A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis.

(c) *Originating agency.* The agency responsible for the initial determination that particular information is classified.

(d) *Multiple sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from more than one source.

(e) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(f) *Special access program.* Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know."

(g) *Intelligence activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(h) *Special activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies, or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(i) *Unauthorized disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

§ 2001.71 Publication and effective date [5.2(c)].

Part 2001 shall be published in the Federal Register. It shall become effective August 1, 1982.

Steven Garfinkel,
Director, Information Security Oversight Office.

June 23, 1982.

[FR Doc. 82-17295 Filed 6-23-82; 10:37 am]
BILLING CODE 6820-AF-M

PART C - SUMMARY OF SPECIFIC POWERS INHERENT IN CLASSIFICATION/DECLASSIFICATION AUTHORITIES

Authorities	Original Classifier			Derivative Classifier			Derivative Declassifier
	TS	S	C	TS	S	C	
Originally classify certain NSI as Top Secret	X						
Originally classify certain NSI as Secret	X	X					
Originally classify certain NSI as Confidential	X	X	X				
Originally declassify certain NSI when also the Original Classifier	X	X	X				
Derivatively classify documents containing RD/FRD/NSI as Top Secret	X			X			
Derivatively classify documents containing RD/FRD/NSI as Secret	X	X		X	X		
Derivatively classify documents containing RD/FRD/NSI as Confidential	X	X	X	X	X	X	
Derivatively declassify documents (RD/FRD/NSI) when also the classifer of the document	X	X	X				
Derivatively declassify certain documents (RD/FRD/NSI) when not the classifier of the document							X

Figure X-1
Powers of Classification/Declassification Authorities

PART D - ORIGINAL CLASSIFICATION OF NATIONAL SECURITY INFORMATION

1. ORIGINAL CLASSIFICATION DETERMINATIONS. An individual with Original Classification Authority may originally classify NSI within the classifier's programmatic jurisdiction at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority whenever classification guidance or relevant classified source documents are not available. The following questions must be answered as part of every original classification determination. Refer to Figure X-1, page X-23, for a summary of this process.

   a. Is the information under consideration for original classification already classified according to a classification guide or a classified source document (e.g., memorandum, formal report)?

      (1) If the answer is "yes", use the classification guide or source document as the original authority for a derivative classification determination (refer to Part E, pages X-29-32 of this Order for instruction on how to make a derivative classification determination).

      (2) If the answer is "no", go on to the next question.

   b. Was the information ever classified as RD or FRD?

      (1) If the answer is "yes", the information is prohibited from being reclassified as NSI (or RD or FRD) by section 146 of the Atomic Energy Act.

      (2) If the answer is "no", go on to the next question.

   c. Does the information concern: (1) military plans, weapons, or operations; (2) the vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security; (3) foreign government information; (4) intelligence activities (including special activities), or intelligence sources or methods; (5) foreign relations or foreign activities of the United States; (6) scientific, technological, or economic matters relating to the national security; (7) U.S. Government programs for safeguarding nuclear materials or facilities; (8) cryptology; (9) a confidential source; or (10) any other category determined by the President or an agency head as requiring protection under Executive Order 12356?

      (1) If the answer is "no", the information cannot be classified, but other restrictions may apply.

      (2) If the answer is "yes", go on to the next question.

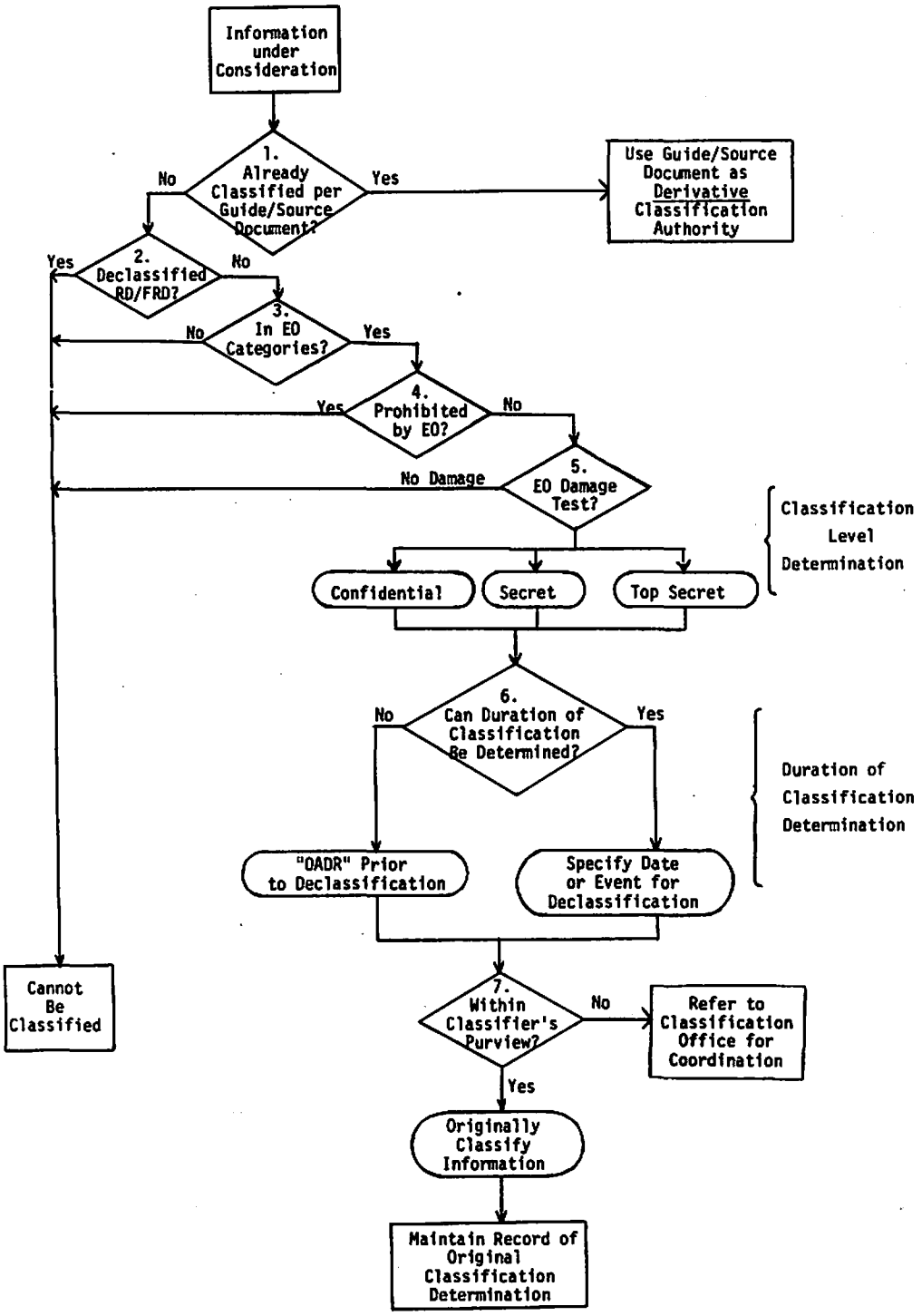


Figure X-2
Original Classification of National Security Information

d. Is the information being proposed for original classification to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security? Does the information concern basic scientific research information not clearly related to the national security?

(1) If the answer to either of the above questions is "yes", the information is prohibited from being classified, but other restrictions may apply.

(2) If the answer to both the above questions is "no", go on to the next question.

e. What degree of damage to the national security could be reasonably expected if the information were not classified?

(1) The following table correlates the degree of damage to the national security that could be reasonably expected if the information were not classified and the classification level that should be assigned to the information.

Degree of Damage	Classification Level
No Damage	Unclassified[1/]
Some Damage	Confidential
Serious Damage	Secret
Exceptionally Grave Damage	Top Secret

(2) If, as indicated in the above table, no damage to the national security could be reasonably expected if the information were not classified, then the information cannot be classified.

(3) If at least some damage to the national security could be reasonably expected if the information were not classified, then the information should be classified at the level indicated in the above table. Go on to the next question.

1/ "Unclassified" is not a classification level but is included here for completeness.

f. Is it possible to specify at the time of original classification a future date or event at which time the information may be declassified?

(1) If the answer is "yes", the date or event for automatic declassification of the information should be specified as part of the original classification determination. Go on to the next question.

(2) If the answer is "no", then the fact that the Originating Agency's Determination (is) Required (OADR) should be specified as part of the original classification determination. This indicates that the information will remain classified until an Authorized Classifier determines that the information may be declassified. (Refer to page VI-1, paragraph 2b, for a description of Derivative Declassification Authority.)

g. Is the information within the classifier's programmatic jurisdiction?

(1) If the answer is "no", the information and the classifier's recommendation as to the level and duration of its classification should be forwarded to the classifier's local classification office or to DP-32, as appropriate, for coordination with the Departmental Element or contractor organization having Original Classification Authority over the information in question.

(2) If the answer is "yes", the information should be classified at the level and for the duration determined above.

2. RECORDKEEPING REQUIREMENTS

a. The Original Classifier shall maintain records of such original decisions so that DP-32 or the responsible Operations Office can periodically review these decisions.

b. Since it is DOE policy to maximize the use of classification guides and minimize the number of original classification decisions, the primary purpose of this review is to assist in the identification of subject areas concerning NSI which require the preparation of formal classification guides. This will allow information identified as NSI by one Original Classifier to be identified by all Original and Derivative Classifiers within DOE, providing consistent and complete protection to the information involved.

PART E - DERIVATIVE CLASSIFICATION DETERMINATIONS

1. AUTHORITY. Individuals with Original or Derivative Classification Authority may derivatively classify documents originated by the classifier or his or her subordinates within the classifier's programmatic jurisdiction that contain RD, FRD, or NSI at any classification level up to and including the level (Top Secret, Secret, Confidential) of the classifier's authority.

2. PROCEDURES. The following questions must be answered as part of every derivative classification determination. Refer to Figure X-3 for a summary of this process. Note that the following process must be repeated for every potentially classified fact or concept in a document.

   a. Does the document or other material under consideration for derivative classification contain or reveal any information, regardless of whether or not it appears to be classified, which is under the programmatic jurisdiction of another agency?

      (1) If the answer is "yes", are applicable source documents or other agency classification guides available and authorized for the classifier's use?

         (a) If so, these guides/source documents shall be used as the basis for making a derivative classification determination for those portions of the document under review under the purview of the other agency.

         (b) If not, the document under review shall be referred to DP-32 for interagency coordination.

      (2) If the answer is "no", go on to the next question.

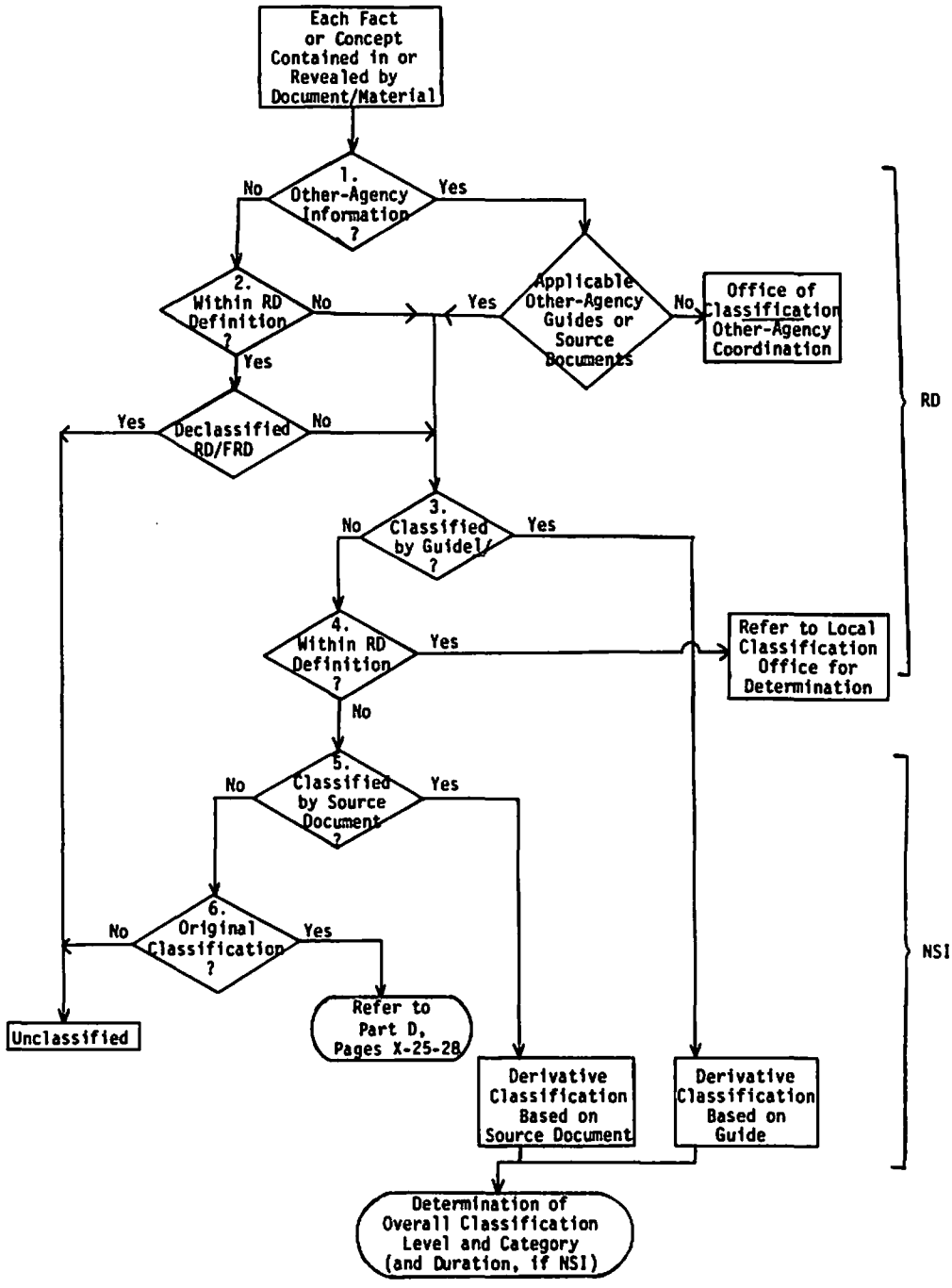
   b. Does the document portion or other material under review contain or reveal information within the scope of the definition of RD?

      (1) If the answer is "yes", does it contain or reveal information that has been specifically and formally removed from the RD category and declassified pursuant to section 142a of the Atomic Energy Act?

         (a) If so, the document portion or other material under review is prohibited from being reclassified as RD, FRD, or NSI by section 146 of the Atomic Energy Act.

         (b) If not, go on to the next question.

      (2) If the answer is "no", go on to the next question.



1/DOE program, local, or other-agency classification guides.

Figure X-3
Derivative Classification of Document or Other Material

c. Can the document portion or other material under review be derivatively classified by use of a DOE program, local, or other agency classification guide authorized for the classifier's use?

(1) If the answer is "yes", the document portion or other material under review shall be derivatively classified at the classification level and category and, if NSI, for the duration specified by the instructions and/or topics in the applicable classification guide. When classifiers are in doubt about the proper interpretation of classification guide topics, they should protect at the higher level and refer the matter promptly to the next higher classification authority. DP-32 is the final authority for determining proper classification.

(2) If the answer is "no", go on to the next question.

d. Does the document portion or other material under review contain or reveal information still within the scope of the definition of RD?

(1) If the answer is "yes", and no applicable guidance exists, the information contained in or revealed by the document or other material under review has not been declassified, and it falls within the definition of RD; therefore, the classification status of the document under review is unclear, and the document should be referred to the local classification office for review and classification. Such documents should be handled as RD pending review.

(2) If the answer is "no", go on to the next question.

e. Can the document portion or other material under review be derivatively classified on the basis of classification of information in a source document which in substance is the same as the information in the document portion or material under review?

(1) If the answer is "yes", the document portion or other material under review shall be derivatively classified at the same classification level and category and, if NSI, for the same duration as that specified in the classified source document. When in doubt about the proper classification of information extracted from a classified source document, a determination should be requested from its classifier. If the classifier cannot be determined, the matter should be referred to the next higher classification authority.

(2) If the answer is "no", go on to the next question.

f. Does the document portion or other material contain or reveal information sufficiently sensitive to be considered for original classification as NSI?

(1) If the answer is "yes", the information in the document should be processed according to the instructions in Attachment 4. An individual with Original Classification Authority must make such a determination.

(2) If the answer is "no", the document portion or other material under review should not be classified, but other restrictions may apply.

g. The above process must be repeated for every potentially classified fact or concept contained in or revealed by a document or other material. Upon completion of the process, the overall classification level and category and, if NSI, the duration of classification of the document or other material can be determined.

(1) The overall classification level of a document or other material is the highest classification level of any information it contains or reveals, regardless of the classification category of that information (Top Secret, higher than Secret, higher than Confidential). (Note: In some subject areas, it is possible that an authoritative compilation from wholly unclassified sources may be classified.)

(2) The overall classification category of a document or other material is the most restrictive classification category of any information it contains or reveals, regardless of the classification level of that information (RD, higher than FRD, higher than NSI).

(3) The duration for which a document or other material is classified is the longest duration of classification for any specific information contained in or revealed by that document or material. Note that no duration of classification is specified for a document in the RD or FRD category, regardless of whether it also contains NSI. For example, a report containing a fact that is Confidential-Restricted Data and another fact that is Secret-National Security Information-Declassify in 10 Years would have an overall classification level and category of Secret-Restricted Data, with no specified declassification date even though no information in the report is classified Secret-Restricted Data.

PART F - DURATION OF CLASSIFICATION CONVERSION TABLE

PREVIOUS EXECUTIVE ORDERS			D 6	D 8	D 10	OADR	DATE OR EVENT
EO 12065	D 6		X				
	REV 20					X	
	REV 30					X	
EO 11652	GDS	TS			X[1/]		
		S		X[1/]			
		C	X				
	XGDS					X	
EO 10501	GROUPS 1, 2, or 3					X	
	GROUP 4	TS			X[1/]		
		S		X[1/]			
		C	X				
DATE OR EVENT							X
NO INDICATION OF DURATION OF CLASSIFICATION						X	

CURRENT EXECUTIVE ORDER (EO 12356)

1/ May be automatically downgraded to the next lower level after two years.

Legend:

D 6 (or 8 or 10) - Declassify 6 (or 8 or 10) years after the date of the document being classified.

OADR - "Originating Agency's Determination Required" prior to the declassification of the document being classified.

REV 20 (or 30) - Review for declassification 20 (or 30) years after the date of the document being classified.

GDS - The document being classified is subject to the "General Declassification Schedule."

XGDS - The document being classified is "Exempt from the General Declassification Schedule."

Groups 1, 2, or 3 - The document being classified is excluded from automatic declassification.

Group 4 - The document being classified is subject to automatic declassification, based on the "General Declassification Schedule."

Date or Event - Declassify upon the occurrence of the specified date or event.

Example: A classification guide indicates that a certain fact is S-NSI-GDS. The document under review should be marked for automatic declassification on a date 8 years after the date of the document (and the document may be automatically downgraded to Confidential 2 years after the date of the document).

Figure X-4
Duration of Classification Conversion Table

PART G - DETERMINATION OF THE CLASSIFICATION OF DOE RESEARCH AND DEVELOPMENT ACTIVITIES

1. RESTRICTED DATA/FORMERLY RESTRICTED DATA. The first step in the evaluation of the classification status of a DOE R&D activity is to determine whether it has the potential for using or generating RD/FRD. Under the Atomic Energy Act, very broad areas of nuclear-related information were originally classified as RD. However, significant amounts of this information have been removed from the RD category pursuant to section 142 of the Atomic Energy Act. Some of this information has been transclassified to FRD (or for certain intelligence information, NSI) and is still under classification control. Some has been declassified. Most specific information that has been transclassified or declassified is identified in DOE program or local guides. General subject areas that have been declassified pursuant to section 142a of the Atomic Energy Act are identified in the "Guide to the Declassified Areas of Nuclear Energy Research" (CG-DAR-1). This guide contains a description of all general R&D subject areas that were once RD/FRD, but which have been declassified. The following questions must be answered as the first step in determining the classification status of any DOE R&D activity. Refer to Figure X-5 for a summary of this process.

   a. Does any part of the activity fall within the scope of the definition of RD?

      (1) If the answer is "no", the activity has virtually no potential for using or generating RD/FRD. Go to step 2, "National Security Information," page X-37.

      (2) If the answer is "yes", go on to the next question.

   b. Does the entire activity fall within the scope of general subject areas that were once RD/FRD, but that are now declassified, as described in CG-DAR-1?

      (1) If the answer is "yes", the activity has virtually no potential for using or generating RD/FRD. Go to step 2, "National Security Information," page X-37.

      (2) If the answer is "no", go on to the next question.

   c. Does the entire activity as currently described fall within the scope of unclassified topics found in DOE program or local classification guides?

      (1) If the answer is "yes", the activity is currently unclassified but has the potential for using or generating RD/FRD because it does not fall within a declassified area of nuclear research. However, in special cases DP-32 may make the determination that it is a Category I activity, provided step 2 of this process does not reveal Category III NSI R&D activity. Go on to step 2.

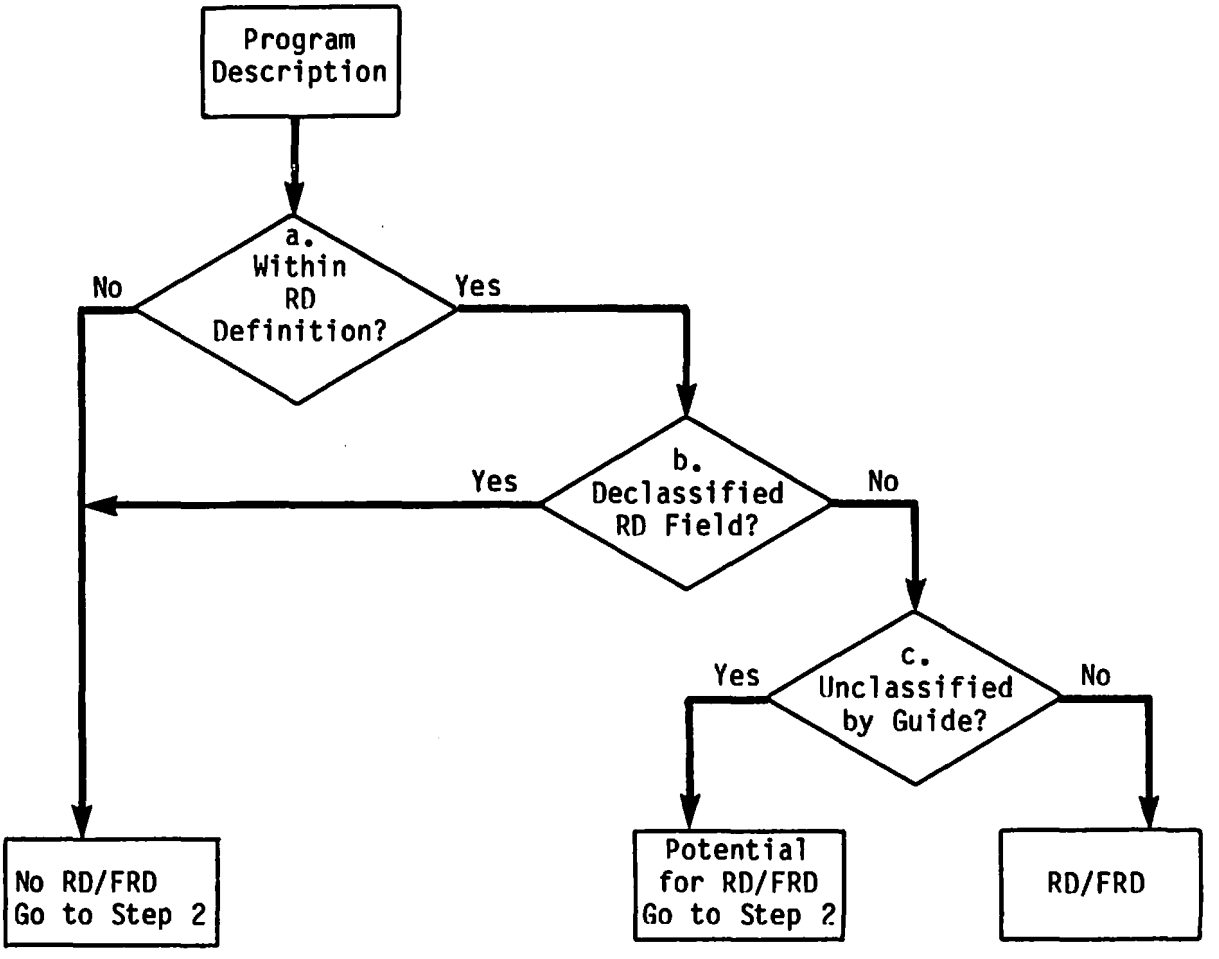


Figure X-5
R&D Activity Classification Status
Step 1 - Restricted Data/Formerly Restricted Data

(2) If the answer is "no", the activity is classified and has a strong potential for using or generating RD/FRD.

2. NATIONAL SECURITY INFORMATION. The second step in the evaluation of the classification status of a DOE R&D activity is to determine whether it has the potential for using or generating NSI that is classified pursuant to Executive Order 12356. Unlike RD, NSI is not classified until an explicit decision is made by someone with the required authority (Original Classification Authority) to determine that it should be classified. The following questions must be answered as the second step in the determination of the classification status of any DOE R&D activity. Refer to Figure X-6 for a summary of this process.

a. Does the activity fall totally within the exclusive programmatic jurisdiction of DOE?

(1) If the answer is "no", the determination of the classification status of the DOE R&D activity under review must be forwarded to DP-32 for possible interagency coordination. (Note: A recommendation should be made concerning the Departmental aspects of the work at the time it is forwarded to DP-32, so proceed to the next question.)

(2) If the answer is "yes", proceed to the next question.

b. Does any part of the activity fall within the scope of classified topics of DOE program or local classification guides?

(1) If the answer is "yes", the activity is classified and has a strong potential for using or generating NSI.

(2) If the answer is "no", the activity is not classified according to current guidance, but consideration should be given to categorizing the activity as having some potential for using or generating NSI. Go on to the next question.

c. Will the activity use or generate only information that has been specifically and formally removed from the RD category and declassified pursuant to section 142a of the Atomic Energy Act?

(1) If the answer is "yes", all information in the activity is prohibited from being reclassified as NSI (or RD or FRD) by section 146 of the Atomic Energy Act and, as a result, the activity belongs in Category I.

(2) If the answer is "no", go on to the next question.

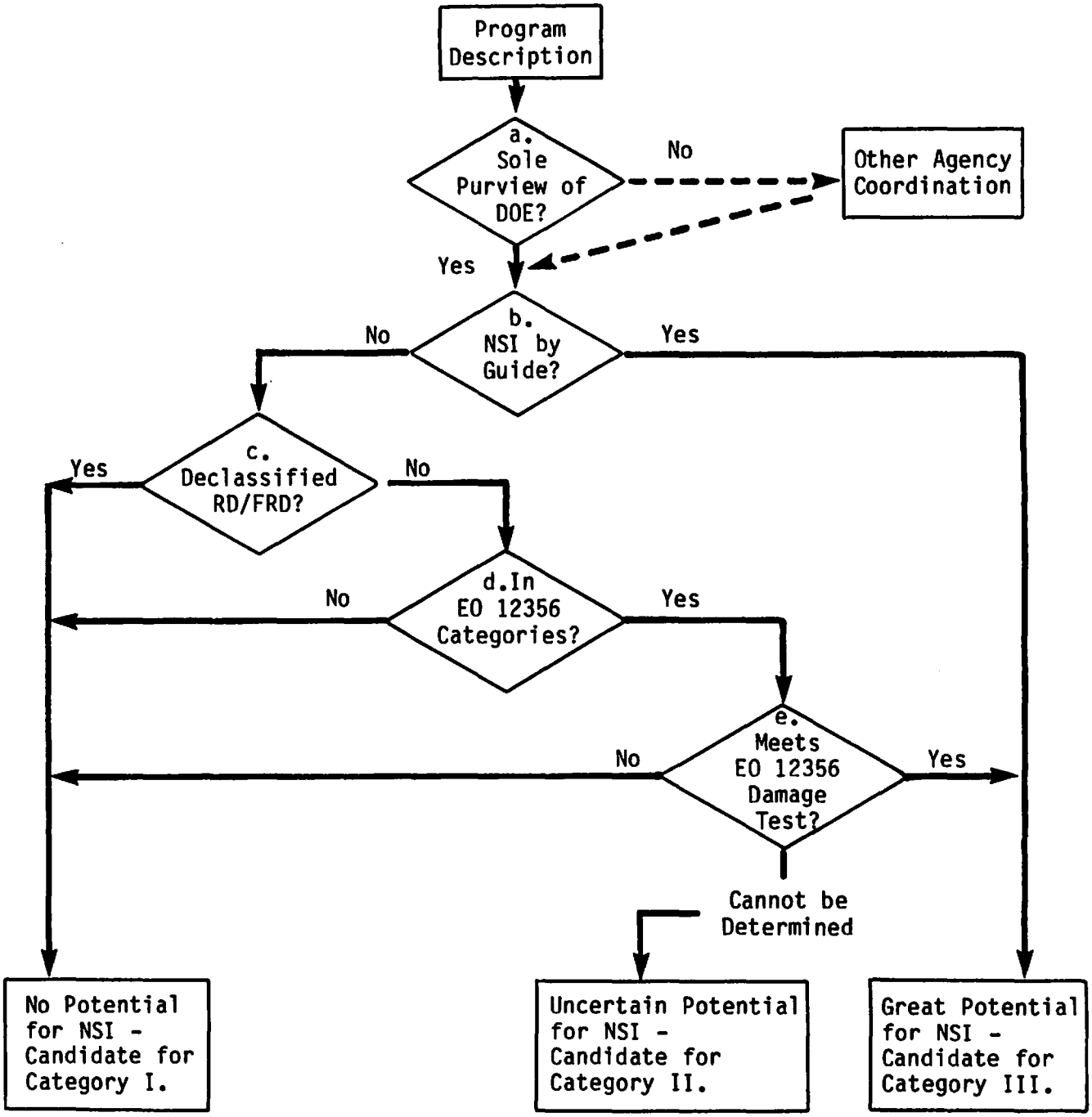


Figure X-6
R&D Activity Classification Status
Step 2 - National Security Information

d. Will the activity use or generate any information that concerns: (1) military plans, weapons, or operations; (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security; (3) foreign government information; (4) intelligence activities (including special activities), or intelligence sources or methods; (5) foreign relations or foreign activities of the United States; (6) scientific, technological, or economic matters relating to the national security; (7) U.S. Government programs for safeguarding nuclear materials or facilities; (8) cryptology; (9) a confidential source; or (10) another category determined by the President or an agency head, or other officials who have been delegated original classification authority by the President, as requiring protection under Executive Order 12356?

(1) If the answer is "no", the activity has virtually no potential for using or generating NSI (unless as determined under the conditions described on page IV-1, paragraph 2a(1)(j)).

(2) If the answer is "yes", go on to the next question.

e. Will the activity use or generate information in the above categories, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security?

(1) If the answer is "no", the activity has virtually no potential for using or generating NSI.

(2) If the answer is "yes", the activity is classified and has great potential for using or generating NSI.

(3) If the answer cannot be determined at this time, the activity still has the potential for using or generating NSI.

3. DETERMINATION OF PROGRAM CLASSIFICATION STATUS CATEGORY. On the basis of the analysis performed in the two steps described above, the third step in determining the classification status category of DOE R&D activities can be performed. Application of Figure X-7 to the results of steps 1 and 2 determines whether a program is in Category I (unclassified), Category II (unclassified, but potentially classified), or Category III (classified).

		FROM STEP 1 - RD/FRD		
		No RD/FRD	Potential for RD/FRD	RD/FRD
FROM STEP 2 NSI	No NSI	I	II	III
	Potential for NSI	II	II	III
	NSI	III	III	III

CATEGORY I ACTIVITY: Unclassified activity with virtually no potential for using or generating classified information.

CATEGORY II ACTIVITY: Unclassified activity with the potential for using or generating classified information.1/

CATEGORY III ACTIVITY: Classified activity with great potential for using or generating classified information.1/

Requirements/Authorities

	Category of DOE R&D Activity		
	I (Unclassified)	II (Potentially Classified)	III (Classified)
a. Category Determination	Heads of HQ or field organization (Director of Classification)		
b. Routine Reporting Requirements	Local Class. Office	Annually to Office of Classification	
c. Recordkeeping Requirements	Local Classification Office/ HQ Program Office		
d. Appointments	None	Derivative Classifier	Classification Officer

NOTE: Refer to text for complete description of table entries.

1/ This is not intended to cover aspects of an activity not directly related to R&D (e.g., facility security).

Figure X-7

R&D Activity Classification Status
Step 3 - Determination of Classification Status Category

INDEX

[1] Subheading can be found as a main heading where more in-depth indexing is provided.

---

2 See Footnote 1.

---

3 See Footnote 1.

Page

---

[4] See Footnote 1.

5 See Footnote 1.

Page