NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Parts 2001 and 2004

RIN 3095–AB18

Classified National Security Information Directive No. 1

AGENCY: Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA).

ACTION: Implementing directive; final rule.

SUMMARY: The Information Security Oversight Office, National Archives and Records Administration, is publishing this Directive as a final rule and pursuant to Section 5.1(a) and (b) of Executive Order 12958, as amended, relating to classified national security information. The Executive order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. 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 classified national security information.

EFFECTIVE DATE: September 22, 2003.

FOR FURTHER INFORMATION CONTACT: J. William Leonard, Director, ISOO, at 202–219–5250.

SUPPLEMENTARY INFORMATION: This final rule is issued pursuant to the provisions of 5.1 (a) and (b) of Executive Order 12958, as further amended by Executive Order 13292, published March 28, 2003 (60 FR 15315) and amends 32 CFR part 2001, Directive No. 1 published on October 13, 1995 (60 FR 53492). Further, this Directive incorporates 32 CFR part 2004, Safeguarding Classified National Security Information, into this Part. The purpose of this Directive is to assist in implementing the Order; users of the Directive shall refer concurrently to that Order for guidance. As of November 17, 1995, ISOO became a part of the National Archives and Records Administration. The Archivist of the United States delegated the implementation and monitoring functions of this program to the Director of ISOO. The drafting, coordination and issuance of this Directive fulfills one of the responsibilities of the implementation delegated to the Director of ISOO.

This rule is being issued as a final rule without prior notice of proposed rulemaking as allowed by the Administrative Procedure Act, 5 U.S.C. 553(b)(3)(A) for rules of agency procedure and interpretation. The interpretive guidance contained in this rule will assist agencies in implementing Executive Order 12958, which was amended on March 25, 2003. NARA has also determined that delaying the effective date for 30 days is unnecessary as this rule updates the existing Directive implementing Executive Order 12958. Moreover, since the revised Executive Order 12958 becomes effective on September 22, 2003, Federal agencies will benefit immediately by having up-to-date ISOO guidance, and any delay in the effective date would hinder agency procedure and be contrary to the public interest.

This rule is not a significant regulatory action for the purposes of Executive Order 12866. This rule is not a major rule as defined in 5 U.S.C. Chapter 8, Congressional Review of Agency Rulemaking. As required by the Regulatory Flexibility Act, we certify that this rule will not have a significant impact on a substantial number of small entities because it applies only to Federal agencies.

List of Subjects

32 CFR Part 2001

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

32 CFR Part 2004

Classified information.

■ 1. Title 32 of the Code of Federal Regulations, part 2001, is revised to read as follows:

PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION

Subpart A—Classification

Sec.

Subpart B—Identification and Markings

Subpart C—Declassification

Subpart D—Safeguarding

Subpart E—Self-Inspections

Subpart F—Security Education and Training

Subpart G—Reporting and Definitions

Authority: Section 5.1(a) and (b), E.O. 12958, 60 FR 19825, 3 CFR 1995 Comp., p. 333, as amended by E.O. 13292, 60 FR 19825, March 25, 2003.

Subpart A—Classification

§ 2001.10 Classification standards [1.1, 1.5].[1]

(a) *''An original classification authority with jurisdiction over the information''* includes:

(1) The official who authorized the original classification, if that official is still serving in the same position;

(2) The originator's current successor in function;

(3) A supervisory official of either; or

(4) The senior agency official under Executive Order 12958, as amended (''the Order'').

(b) *''Permanently valuable information''* or *''permanent historical value''* refers to information contained in:

(1) Records that have been accessioned into the National Archives of the United States;

(2) Records that have been scheduled as permanent under a records

[1] Bracketed references pertain to related sections of Executive Order 12958, as amended by E.O. 13292.

disposition schedule approved by the National Archives and Records Administration (NARA); and

(3) Presidential historical materials, presidential records or donated historical materials located in the National Archives of the United States, a presidential library, or any other approved repository.

(c) *Identifying or describing damage to the national security.* Section 1.1(a) of the Order sets forth the conditions for classifying information in the first instance. One of these conditions, the ability to identify or describe the damage to the national security, is critical to the process of making an original classification decision. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

(d) *Declassification without proper authority.* Classified information that has been declassified without proper authority remains classified. Administrative action shall be taken to restore markings and controls, as appropriate.

§ 2001.11 Classification authority [1.3].

(a) *General.* Agencies with original classification authority shall establish a training program for original classifiers in accordance with subpart F of this part.

(b) *Requests for original classification authority.* Agencies not possessing such authority shall forward requests to the Director of the Information Security Oversight Office (ISOO). The agency head must make the request and shall provide a specific justification of the need for this authority. The Director of ISOO shall forward the request, along with the Director's recommendation, to the President through the Assistant to the President for National Security Affairs within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the procedures of this section.

§ 2001.12 Duration of classification [1.5].

(a) *Determining duration of classification for information originally classified under the Order.*

(1) *Establishing duration of classification.* When determining the duration of classification for information originally classified under this Order, an original classification authority shall follow the sequence listed in paragraphs (a)(1)(i), (ii), and (iii) of this section.

(i) The original classification authority shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

(ii) If unable to determine a date or event of less than 10 years, the original classification authority shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(iii) If unable to determine a date or event of 10 years, the original classification authority shall assign a declassification date not to exceed 25 years from the date of the original classification decision.

(2) *Extending duration of classification for information originally classified under the Order.* Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event. If an original classification authority has assigned a date or event for declassification that is less than 25 years from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origination.

(i) For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information's origin. Continued classification of this information beyond 25 years is governed by section 3.3 of the Order.

(ii) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition of those records (destruction date) in each agency Records Control Schedule or General Records Schedule approved by the National Archives and Records Administration, although the duration of classification may be extended if a record has been retained for business reasons beyond its scheduled destruction date.

(iii) For currently unscheduled records, the duration of classification beyond 25 years shall be determined in accordance with the provisions of (a)(2)(i) (for permanently valuable records) or (a)(2)(ii) (for temporary records) when the records are scheduled.

(3) *Conditions for extending classification.* When extending the duration of classification, the original classification authority must:

(i) Be an original classification authority with jurisdiction over the information;

(ii) Ensure that the information continues to meet the standards for classification under the Order; and

(iii) Make reasonable attempts to notify all known holders of the information.

(b) *Information classified under prior orders.*

(1) *Specific date or event.* Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. However, if the information is contained in records determined by the Archivist of the United States to be permanently valuable, and the prescribed date or event will take place more than 25 years from the information's origin, the declassification of the information will instead be subject to section 3.3 of the Order.

(2) *Indefinite duration of classification.* For information marked ''Originating Agency's Determination Required,'' its acronym ''OADR,'' or with some other marking indicating an indefinite duration of classification under a prior order:

(i) A declassification authority, as defined in section 6.1 of the Order, may declassify it;

(ii) An authorized original classification authority with jurisdiction over the information may re-mark the information to establish a duration of classification consistent with the requirements for information originally classified under the Order, as provided in paragraph (a) of this section; or

(iii) Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.3 of the Order.

(c) *Changing the classification level of information originally classified under the Order.* An original classification authority with jurisdiction over the information may change the level of classification of information. Documents shall be remarked with the new classification level, the date of the

action, and the authority for the change. Changing the classification level may also require changing portion markings for information contained within a document. Additionally, the original classification authority shall update appropriate security classification guides.

(d) *Reclassifying specific information.* An original classification authority with jurisdiction over the information may reclassify information that has been declassified or marked as unclassified in cases involving specific information that has not been publicly released under proper authority and has not been subject to a Freedom of Information Act, Privacy Act, or Mandatory Declassification Review request. (If the information has been publicly released under proper authority, see section 1.7(c) of the Order and § 2001.13; if the information has not been publicly released but has been the subject of an access demand, see section 1.7(d) of the Order.).

(1) When taking this action, an original classification authority must include the following markings on the information:

(i) The level of classification;

(ii) The identity, by name or personal identifier and position, of the original classification authority;

(iii) declassification instructions;

(iv) a concise reason for classification; and

(v) the date the action was taken.

(2) The original classification authority shall notify all known authorized holders of this action.

(e) *Exemption categories from 10-year declassification.* The markings for exemption categories X1 through X8 can no longer be used. When these markings appear on information dated before September 22, 2003, the information shall be declassified 25 years from the date of the original decision, unless it has been properly exempted under section 3.3 of the Order.

(f) *Foreign government information.* The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. Depending on the age of the information and whether it is contained in permanently valuable records, the declassifying agency shall also determine if another exemption under section 3.3 (b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

(g) *Determining when information is subject to automatic declassification.* The ''date of the information's origin'' or ''the information's origin,'' as used in the Order and this part, pertains to the date that specific information, which is contemporaneously or subsequently classified, is first recorded in an agency's records, or in presidential historical materials, presidential records or donated historical materials. The following examples illustrate this process:

Example 1. An agency first issues a classification guide on the F–99 aircraft on October 20, 1995. The guide states that the fact that the F–99 aircraft has a maximum velocity of 500 m.p.h. shall be classified at the ''Secret'' level for a period of ten years. A document dated July 10, 1999, is classified because it includes the maximum velocity of the F–99. The document should be marked for declassification on October 20, 2005, ten years after the specific information was first recorded in the guide, not on July 10, 2009, ten years after the derivatively classified document was created.

Example 2. An agency classification guide issued on October 20, 1995, states that the maximum velocity of any fighter aircraft shall be classified at the ''Secret'' level for a period of ten years. The agency first records the specific maximum velocity of the new F–88 aircraft on July 10, 1999. The document should be marked for declassification on July 10, 2009, ten years after the specific information is first recorded, and not on October 20, 2005, ten years after the date of the guide's generic instruction. Subsequent documents containing this information would be marked for declassification 10 years from the date of the document.

§ 2001.13 Classification prohibitions and limitations [1.7].

(a) In making the decision to reclassify information that has been declassified and released to the public under proper authority, the agency head or deputy agency head must determine in writing that reclassification of the information is necessary in the interest of the national security.

(1) In addition, the agency must deem the information to be reasonably recoverable which means that:

(i) Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from them and

(ii) If the information has been made available to the public via means such as Government archives or reading rooms, it is withdrawn from public access.

(2) The declassification and release of information under proper authority means that the agency originating the information authorized the declassification and release of the information.

(b) Once the reclassification action has occurred, it must be reported to ISOO within 30 days. The notification must include how the ''reasonably recoverable'' decision was made, including the number of recipients or holders, how the information was retrieved and how the recipients or holders were briefed.

(c) Any recipients or holders of the reclassified information who have current security clearances shall be appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holders who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to, their obligation not to disclose the information, and be requested to sign an acknowledgement of this briefing.

(d) The reclassified information must be appropriately marked and safeguarded. The markings should include the reclassification authority and the date of the action. Apply other markings as provided in subpart B of this part.

§ 2001.14 Classification challenges [1.8].

(a) *Challenging classification.* Authorized holders wishing to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific classified information in accordance with the provisions of the Order to include the special conditions set forth in section 4.1(h) of the Order. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

(b) *Agency procedures.* (1) Because the Order encourages authorized holders to challenge classification as a means for promoting proper and thoughtful classification actions,

agencies shall ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

(2) Agencies shall establish a system for processing, tracking and recording formal classification challenges made by authorized holders. Agencies shall consider classification challenges separately from Freedom of Information Act or other access requests, and shall not process such challenges in turn with pending access requests.

(3) The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond to the challenge within 60 days, the agency must acknowledge the challenge in writing, and provide a date by which the agency will respond. The acknowledgment must include a statement that if no agency response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision. The challenger may also forward the challenge to the ISCAP if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. Agency responses to those challenges it denies shall include the challenger's appeal rights to the ISCAP.

(4) Whenever an agency receives a classification challenge to information that has been the subject of a challenge within the past two years, or that is the subject of pending litigation, the agency is not required to process the challenge beyond informing the challenger of this fact and of the challenger's appeal rights, if any.

(c) *Additional considerations.* (1) Challengers and agencies shall attempt to keep all challenges, appeals and responses unclassified. However, classified information contained in a challenge, an agency response, or an appeal shall be handled and protected in accordance with the Order and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

(2) The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be encouraged as a means of holding down the number of formal challenges.

§ 2001.15 Classification guides [2.2].

(a) *Preparation of classification guides.* Originators of classification guides are encouraged to consult users of guides for input when developing or updating guides. When possible, originators of classification guides are encouraged to communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure the consistency and uniformity of classification decisions. Each agency shall maintain a list of its classification guides in use.

(b) *General content of classification guides.* Classification guides shall, at a minimum:

(1) Identify the subject matter of the classification guide;

(2) Identify the original classification authority by name or personal identifier, and position;

(3) Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;

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

(5) State precisely the elements of information to be protected;

(6) State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;

(7) State, when applicable, special handling caveats;

(8) Prescribe declassification instructions or the exemption category from automatic declassification at 25 years, as approved by the ISCAP under section 3.3(d) of the Order and listed in § 2001.21(e) of subpart B, for each element of information; and

(9) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.4 of the Order.

(c) Dissemination of classification guides. Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.

(d) *Reviewing and updating classification guides.*

(1) Classification guides, including guides created under prior orders, shall be reviewed and updated as circumstances require, but, in any event, at least once every five years. Updated instructions for guides first created under prior orders shall comply with the requirements of the Order and this part.

(2) Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. Also, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide.

Subpart B—Identification and Markings

§ 2001.20 General [1.6].

A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after September 22, 2003, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

§ 2001.21 Original classification [1.6(a)].

(a) *Primary markings.* On the face of each originally classified document, regardless of the media, the original classification authority shall apply the following markings.

(1) *Classification authority.* The name or personal identifier, and position title of the original classification authority shall appear on the ''Classified By'' line. An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

or

Classified By: ID#IMNO1, Chief, Division 5, Department of Good Works, Office of Administration

(2) *Agency and office of origin.* If not otherwise evident, the agency and office of origin shall be identified and follow the name on the ''Classified By'' line. An example might appear as:

Classified By: David Smith, Chief, Division 5 Department of Good Works, Office of Administration.

(3) *Reason for classification.* The original classification authority shall identify the reason(s) for the decision to classify. The original classification authority shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.4 plus the letter(s) that corresponds to that classification category in section 1.4 of the Order.

(i) These categories, as they appear in the Order, are as follows:

(A) Military plans, weapons systems, or operations;

(B) Foreign government information;

(C) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(D) Foreign relations or foreign activities of the United States, including confidential sources;

(E) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

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

(G) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(H) Weapons of mass destruction.

(ii) An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: Vulnerabilities or capabilities of plans relating to the national security

or

Reason: 1.4(g)

(iii) When the reason for classification is not apparent from the content of the information, *e.g.*, classification by compilation, the original classification authority shall provide a more detailed explanation of the reason for classification.

(4) *Declassification instructions.* The duration of the original classification decision shall be placed on the ''Declassify On'' line. The original classification authority will apply one of the following instructions:

(i) The original classification authority will apply a date or event for declassification that corresponds to the lapse of the information's national security sensitivity, that is less than 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: October 14, 2004

or

Declassify On: Completion of Operation

(ii) When a specific date or event within 10 years cannot be established, the original classification authority will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 2003, mark the ''Declassify On'' line as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: October 14, 2013

(iii) Upon the determination that the information must remain classified beyond 10 years, the original classification authority will apply a date not to exceed 25 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2003, mark the ''Declassify On'' line as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: October 10, 2028

(b) Overall marking. The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text.

(1) Conspicuously place the overall classification 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) For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked ''Secret'' and other information marked ''Confidential,'' the overall marking would be ''Secret.''

(3) Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation ''Unclassified'' when it is applicable, or with the highest overall classification of the document.

(c) *Portion marking.* Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

(1) To indicate the appropriate classification level, the symbols ''(TS)'' for Top Secret, ''(S)'' for Secret, ''(C)'' for Confidential, and ''(U)'' for Unclassified shall be used.

(2) Each classified portion of a document marked exempt from automatic declassification shall be exempted unless the original classification authority indicates otherwise on the document.

(3) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information. Such a request shall be submitted to the Director of ISOO and should include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

(d) *Classification extensions.* (1) An original classification authority may extend the duration of classification for up to 25 years from the date of the information's origin for information contained in records determined to be permanently valuable.

(2) The ''Declassify On'' line shall be revised to include the new declassification instructions, and shall include the identity of the person authorizing the extension and the date of the action.

(3) The office of origin shall make reasonable attempts to notify all holders of such information. Classification guides shall be updated to reflect such revisions.

(4) An example of an extended duration of classification may appear as follows for a document dated December 1, 2003 with a declassification date of December 1, 2015:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: Classification extended on December 1, 2005, until December 1, 2028, by David Jones, Chief, Division 5

(e) *Marking information exempted from automatic declassification at 25 years.* (1) When an agency head or senior agency official exempts permanently valuable information from automatic declassification at 25 years, the ''Declassify On'' line shall be revised to include the symbol ''25X'' plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.3(b) of the Order. Other than when the exemption pertains to the identity of a confidential human source, or a human intelligence source, the revised ''Declassify On'' line shall also include the new date or event for declassification. The marking for an exemption for the identity of a confidential human source or a human intelligence source shall be ''25X1-human.'' This marking denotes that this specific information is not subject to automatic declassification.

(2) The pertinent exemptions, using the language of section 3.3(b) of the Order, are:

25X1: reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

25X2: reveal information that would assist in the development or use of weapons of mass destruction;

25X3: reveal information that would impair U.S. cryptologic systems or activities;

25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

25X5: reveal actual U.S. military war plans that remain in effect;

25X6: reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

25X9: violate a statute, treaty, or international agreement.

(3) The pertinent portion of the marking would appear as:

Declassify On: 25X-State-of-the-art technology within a U.S. weapon system, October 1, 2020

or

Declassify On: 25X4, October 1, 2020

(4) Documents should not be marked with a ''25X'' marking until the agency has been informed that the President or the Interagency Security Classification Appeals Panel concurs with the proposed exemption. Agencies that have submitted proposed exemptions or a declassification guide to the ISCAP may mark documents with ''25X'' categories, while waiting for ISCAP concurrence, unless otherwise notified by the Panel's Executive Secretary.

(5) Agencies need not apply a ''25X'' marking to individual documents contained in a file series exempted from automatic declassification under section 3.3(c) of the Order until the individual document is removed from the file.

§ 2001.22 Derivative classification [2.1].

(a) *General.* Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.20 and § 2001.21, except as provided in this section. Information for these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

(b) *Source of derivative classification.* (1) The derivative classifier shall concisely identify the source document or the classification guide on the ''Derived From'' line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as:

Derived From: Memo, ''Funding Problems,'' October 20, 2003, Office of Administration, Department of Good Works

or

Derived From: CG No. 1, Department of Good Works, dated October 20, 2003

(i) When a document is classified derivatively on the basis of more than one source document or classification guide, the ''Derived From'' line shall appear as: Derived From: Multiple Sources

(ii) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. When practicable, this list should be included in or with all copies of the derivatively classified document.

(2) A document derivatively classified on the basis of a source document that is itself marked ''Multiple Sources'' shall cite the source document on its ''Derived From'' line rather than the term ''Multiple Sources.'' An example might appear as:

Derived From: Report entitled, ''New Weapons,'' dated October 20, 2003, Department of Good Works, Office of Administration

(c) *Reason for classification.* The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not required to be transferred in a derivative classification action. If included, however, it shall conform to the standards in § 2001.21(a)(3).

(d) *Declassification instructions.* (1) The derivative classifier shall carry forward the instructions on the ''Declassify On'' line from the source document to the derivative document, or the duration instruction from the classification or declassification guide.

(2) When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the ''Declassify On'' line shall reflect the longest duration of any of its sources.

(i) When a document is classified derivatively either from a source document(s) or a classification guide that contains the declassification instruction, ''Originating Agency's Determination Required,'' or ''OADR,'' or from a source document(s) or a classification guide that contains any of the exemption markings X1 through X8. Unless otherwise instructed by the original classifier, the derivative classifier shall carry forward:

(A) The fact that the source document(s) was marked with this instruction; and

(B) The date of origin of the most recent source document(s), classification guides, or specific information, as appropriate to the circumstances.

(ii) Examples might appear as:

Declassify On: Source Marked ''OADR'', Date of source: October 20, 1990

or

Declassify On: Source Marked ''X1'', Date of source: October 20, 2000

(iii) Either of these markings will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under section 3.3 of the Order.

(e) *Overall marking.* The derivative classifier shall conspicuously mark the classified document with the highest level of classification of information included in the document, as provided in § 2001.21(b).

(f) *Portion marking.* Each portion of a derivatively classified document shall be marked in accordance with its source, and as provided in § 2001.21(c).

§ 2001.23 Additional requirements [1.6].

(a) *Marking prohibitions.* Markings other than ''Top Secret,'' ''Secret,'' and ''Confidential,'' such as ''For Official Use Only,'' ''Sensitive But Unclassified,'' ''Limited Official Use,'' or ''Sensitive Security Information'' shall not be used to identify classified 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 classified national security information. The terms ''Top Secret,'' ''Secret,'' and ''Confidential'' should not be used to identify non-classified executive branch information.

(b) *Agency prescribed special markings.* Agencies shall refrain from the use of special markings when they merely restate or emphasize the principles and standards of the Order and this part. Upon request, the senior agency official shall provide the Director of ISOO with a written explanation for the use of agency special markings.

(c) *Transmittal documents.* A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal shall also include conspicuously on its face the following or similar instructions, as appropriate:

Unclassified When Classified Enclosure Removed

or

Upon Removal of Attachments, This Document is (Classification Level)

(d) *Foreign government information.* Documents that contain foreign government information shall include the marking, ''This Document Contains (indicate country of origin) Information.'' The portions of the document that contain the foreign government information shall be marked to indicate the government and classification level, using accepted country code standards, *e.g.*, ''(Country code—C).'' If the identity of the specific government must be concealed, the document shall be marked, ''This Document Contains Foreign Government Information,'' and pertinent portions shall be marked ''FGI'' together with the classification level, *e.g.*, ''(FGI–C).'' In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. When classified records are transferred to the National Archives and Records Administration for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information. If the fact that information is foreign government information must be concealed, the markings described in this paragraph shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(e) *Working papers.* A working paper is defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and if otherwise appropriate, destroyed when no longer needed. When any of the following conditions applies, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

(1) Released by the originator outside the originating activity;

(2) Retained more than 180 days from the date of origin; or

(3) Filed permanently.

(f) *Other material.* Bulky material, equipment and facilities, etc. shall be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility.

(g) *Unmarked materials.* Information contained in unmarked records, or presidential or related materials, and which pertains to the national defense or foreign relations of the United States and has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under the Order, and is subject to its provisions regarding declassification.

§ 2001.24 Declassification markings [1.5, 1.6, 3.3].

(a) *General.* A uniform security classification system requires that standard markings be applied to declassified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of declassified information shall not deviate from the following prescribed formats. If declassification markings cannot be affixed to specific information or materials, (*e.g.*, agencies using automated information systems, special media, microfilm) the originator shall provide holders or recipients of the information with written instructions for marking the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the declassified status of the information and who authorized the declassification.

(b) The following markings shall be applied to records, or copies of records, regardless of media:

(1) The word, ''Declassified;''

(2) The name or personal identifier, and position title of the declassification authority or declassification guide;

(3) The date of declassification; and

(4) The overall classification markings that appear on the cover page or first page shall be lined with an ''X'' or straight line. An example might appear as:

~~**SECRET**~~

Declassified by David Smith, Chief, Division 5, August 17, 2005

Subpart C—Declassification

§ 2001.30 Automatic declassification [3.3].

(a) *General.* All departments and agencies that have original classification authority, or previously had original classification authority, and maintain records appraised as having permanent historical value that contain information classified by that agency shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in managing automatic declassification of accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States.

(b) *Presidential records.* The Archivist of the United States shall establish procedures for the declassification of presidential or White House materials transferred to the legal custody of the National Archives of the United States or maintained in the presidential libraries.

(c) *Classified information in the custody of contractors, licensees, certificate holders, grantees or other authorized private organizations or individuals.* Pursuant to the provisions of National Industrial Security Program, agencies must provide security classification/declassification guidance to such entities or individuals who possess classified information. Agencies must also determine if classified Federal records are held by such entities or individuals, and if so, whether they are permanent records of historical value and thus subject to section 3.3 of this Order. Until such a determination has been made by an appropriate agency official, the classified information contained in such records shall not be subject to automatic declassification and shall be safeguarded in accordance with the most recent security classification/declassification guidance provided by the agency.

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

(e) *Unofficially transferred information.* In the case of classified information that is not officially transferred as described in paragraph (d), of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, the Director of ISOO will designate an agency or agencies to act on provisions of the Order, with the concurrence of the designated agency or agencies.

(f) *Processing records originated by another agency.* When an agency uncovers classified records originated by another agency that appear to meet the criteria for the application of the automatic declassification provisions of the Order, the finding agency should

alert the originating agency and seek instruction.

(g) *Unscheduled records.* Classified information in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.3 of the Order. Classified information in records that are scheduled as permanently valuable when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 3.3 of the Order five years from the date the records are scheduled. Classified information in records that are scheduled as permanently valuable when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 3.3 of the Order when the information is 25 years old.

(h) *Foreign government information.* The declassifying agency is the agency that initially received or classified the information. When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency shall also determine if another exemption under section 3.3(b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

(i) *Assistance to the Archivist of the United States.* Agencies shall consult with NARA before establishing automatic declassification programs. Agencies shall cooperate with NARA in developing schedules for the declassification of records in the National Archives of the United States and the presidential libraries to ensure that declassification is accomplished in a timely manner. NARA will provide information about the records proposed for automatic declassification. Agencies shall consult with NARA before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate information about agency declassification actions when records are accessioned into NARA. NARA will provide guidance to the agencies about the requirements for notification of declassification actions on accessioned records, box labeling, and identifying exempt information in the records.

(j) *Use of approved declassification guides.* Approved declassification guides are a basis for the exemption from automatic declassification of specific information as provided in section 3.3(d) of the Order. These guides must include additional pertinent detail relating to the exemptions described in section 3.3(b) of the Order, and follow the format required of declassification guides for systematic review as described in § 2001.32 of this part. In order for such guides to be used in place of the identification of specific information within individual documents, the information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions for general categories of information will not be acceptable. The actual items to be exempted are specific documents. All such declassification guides used in conjunction with section 3.3(d) of the Order must be submitted to the Director of ISOO, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, for approval by the Panel.

(k) *Automatic declassification date.* No later than December 31, 2006, all classified records that are more than 25 years old and have been determined to have permanent historical value will be automatically declassified whether or not the records have been reviewed.

(l) *Exemption from Automatic Declassification.* Agencies may propose to exempt from automatic declassification specific information, either by reference to information in specific records or in the form of a classification or declassification guide, within five years of, but not later than 180 days before the information is subject to automatic declassification. The agency head or senior agency official, within the specified timeframe, shall notify the Director of ISOO, serving as the Executive Secretary of the Interagency Security Classification Appeals Panel, of the specific information being proposed for exemption from automatic declassification.

(m) *Delays in the onset of automatic declassification.* (1) Microforms, motion pictures, audiotapes, videotapes, or comparable media. An agency head or senior agency official, either through its agency's declassification plan, or within 90 days of the decision, must notify the Director of the Information Security Oversight Office of a decision to delay the onset of automatic declassification for classified information contained in this type of media. Agencies may delay the date for automatic declassification for up to five additional years for these types of special media. Information contained in special media that has been referred shall be automatically declassified five years from the date of notification or 30 years from the date of origination of the special media, whichever is longer, unless the information has been properly exempted by the equity holding agency under section 3.3(d) of the Order.

(2) Referred or Transferred Records. An agency head or senior agency official, either through the agency's declassification plan or within 90 days of the decision, must notify the Director of the Information Security Oversight Office of a decision to delay the onset of automatic declassification for records that have been referred or transferred to that agency. Agencies that have records subject to automatic declassification must identify all equities and refer them to the appropriate agency prior to the date of automatic declassification or, if the information has been properly exempted by the referring agency, prior to the specific date or event for declassification under section 3.3(d) of the Order. Information contained in records that have been referred shall be automatically declassified three years from the date of notification or 28 years from the date of origination of the records, whichever is longer, unless the information has been properly exempted by another equity holding agency under section 3.3(d) of the Order. Agencies receiving a notification of a referral must immediately acknowledge receipt of it. Notifying agencies must follow-up if an acknowledgment is not received within 60 days.

(3) Newly Discovered Records. An agency head or senior agency official must notify the Director of the Information Security Oversight Office of any decision to delay automatic declassification no later than 90 days, from discovery of the records. The notification should identify the records and the anticipated date for declassification. An agency has up to three years from the date of discovery to make a declassification, exemption or referral determination. If other agencies' interests or equities are identified in the newly discovered records, those agencies will have three years from the date of notification to complete their review and make a declassification or exemption determination.

(n) *Redaction standard.* Agencies are encouraged but are not required to redact documents that contain information that is exempt from

automatic declassification under section 3.3 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document.

(o) *Restricted Data and Formerly Restricted Data.* (1) Records containing Restricted Data (RD) and Formerly Restricted Data (FRD) are excluded from the automatic declassification requirements in section 3.3 of the Order because they are classified under the Atomic Energy Act of 1954, as amended. Restricted Data concerns:

(i) The design, manufacture, or utilization of atomic weapons;

(ii) The production of special nuclear material, *e.g.*, enriched uranium or plutonium; or

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

(2) Formerly Restricted Data is information that is still classified but which has been removed from the Restricted Data category because it is related primarily to the military utilization of atomic weapons.

(3) Any document marked as containing Restricted Data or Formerly Restricted Data shall remain classified indefinitely or shall be referred to the Department of Energy for a classification review.

§ 2001.31 Systematic declassification review [3.4].

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

(b) *Responsibilities.* Agencies shall establish systematic review programs for those records containing information exempt from automatic declassification. Agencies may also conduct systematic review of information contained in permanently valuable records that is less than 25 years.

§ 2001.32 Declassification guides [3.3].

(a) *Preparation of declassification guides.* Declassification guides shall be prepared to facilitate the declassification of information contained in records determined to be of permanent historical value. When it is sufficiently detailed and understandable, and identified for both purposes, a classification guide may also be used as a declassification guide.

(b) *General content of declassification guides.* Declassification guides shall, at a minimum:

(1) Identify the subject matter of the declassification guide;

(2) Identify the original declassification authority by name or personal identifier, and position;

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

(4) State precisely the categories or elements of information:

(i) To be declassified;

(ii) To be downgraded; or

(iii) Not to be declassified.

(5) Identify any related files series that have been exempted from automatic declassification pursuant to section 3.3(c) of the Order;

(6) To the extent a guide is used in conjunction with the automatic declassification provisions in section 3.3 of the Order, state precisely the elements of information to be exempted from declassification to include:

(i) The appropriate exemption category listed in section 3.3(b) of the Order, and, when citing the exemption category listed in section 3.3(b)(9) of the Order, specify the applicable statute, treaty or international agreement; and

(ii) A date or event for declassification.

(c) *External review.* Agencies shall submit declassification guides for review to the Director of ISOO. To the extent such guides are used in conjunction with the automatic declassification provisions in section 3.3 of the Order, the Director shall submit them for approval by the Interagency Security Classification Appeals Panel. Agencies that have submitted a declassification guide to the ISCAP may use the guide while waiting for ISCAP approval, unless otherwise notified by the Panel's Executive Secretary.

(d) *Internal review and update.* Agency declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. Each agency shall maintain a list of its declassification guides in use.

§ 2001.33 Mandatory review for declassification [3.5, 3.6].

(a) *U.S. originated information.*

(1) Receipt of requests. Each agency shall publish in the **Federal Register** the identity of the person(s) or office(s) to which mandatory declassification review requests should 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 specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. 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 ordinarily make a final determination within one year from the date of receipt. When information cannot be declassified in its entirety, agencies shall make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon 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 refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall process the request in accordance with this section. 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 60 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.

(iv) Appeals to the Interagency Security Classification Appeals Panel. In accordance with section 5.3(c) of the Order, the Interagency Security Classification Appeals Panel shall publish in the **Federal Register** the rules and procedures for bringing mandatory declassification appeals before it.

(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 this section. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

(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 9701 of title 31, United States Code.

(e) *Assistance to the Department of State.* 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 materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

(f) *Requests filed under mandatory declassification review and the Freedom of Information Act.* When a requester submits a request both under mandatory review and the Freedom of Information Act (FOIA), the agency shall require the requester to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory review.

(g) *FOIA and Privacy Act requests.* Agency heads shall process requests for declassification that are submitted under the provisions of the FOIA, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

(h) *Redaction standard.* Agencies shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction.

§ 2001.34 Referrals [3.3, 3.6].

(a) *Approaches to declassification.* The exchange of information between agencies and the final disposition of documents are affected by differences in the approaches to declassification. To facilitate this process, the Information Security Oversight Office, in coordination with the National Archives and Records Administration and the other concerned agencies, shall standardize the referral process, including the development of standard forms. Agencies conducting pass/fail reviews may refer documents to agencies that redact. Actions taken by the sender and the recipient may differ as noted below:

(1) When a referral is from a pass/fail agency to a pass/fail agency, both agencies conduct a pass/fail review and annotate the classification or declassification decisions in accordance with NARA guidelines. The receiving agency should also notify the referring agency that the review has been completed.

(2) When a referral is from a pass/fail agency to a redaction agency, the redaction agency is only required to conduct pass/fail reviews of documents referred by a pass/fail agency. If the redaction agency wishes to redact the document, it must do so on a copy of the referred document, then file the redacted version with the original. The redaction agency should also notify the pass/fail referring agency that the review has been completed.

(3) Referrals from redaction agencies to pass/fail agencies will be in the form of document copies. In the course of review the pass/fail agency may either pass or fail the document or its equities. The pass/fail agency may review and redact failed documents when practicable.

(4) Referrals between redaction agencies may result in redaction of any exemptible equities.

(b) *Referral decisions.* When agencies review documents or folders only to the point at which exemptible information is identified, they must take one of the following actions to protect any other unidentified equities that may be in the unreviewed portions of the document:

(1) Complete a review of the document or folder to identify other agency equities and notify those agencies; or

(2) Exempt the document or folder and assign a Date/Event for automatic declassification, before which time they must provide timely notification to any equity agencies. Agencies reviewing a previously exempted document or folder may apply a different exemption and new Date/Event for automatic declassification based upon the content of previously unreviewed equities.

(c) *Unmarked or improperly marked documents.* Agencies that find other agency information in unmarked or improperly marked documents may apply a different exemption and new Date/Event for automatic declassification based upon the content of previously unreviewed equities.

(d) *Means of Referral.* The reviewing agency must communicate referrals to equity agencies. They may use either of the methods below:

(1) Full text referral. Agencies will make referrals in a format mutually agreed to by the referring and receiving agencies. Each referral request will clearly identify the referring agency and may identify the sections or areas of the document containing the receiving agency's equities and the requested action; or

(2) Tab and notify.

(i) Agencies will use NARA-approved tabs and will clearly indicate on them the agency or agencies having equity in the document(s) held within the tabs. Successive documents with identical equity(ies) may be grouped within a single tab. Documents with differing equities, or non-successive documents, must be tabbed individually. In general, document order may not be changed to facilitate tabbing. In cases where there are so many tabbed documents in a box that tabbing documents individually would seriously overfill the box, the reviewer may group documents under a single tab for each agency equity at the back of each file folder, or back of the box if there is no file folder. If this becomes necessary, the reviewer shall prepare a folder/document list or consult with NARA so that original order can be restored during archival processing.

(ii) Agency notification must include, at a minimum, the following information: the approximate volume of equity, the highest classification of documents, the exact location (to box level) of the documents so marked, and instructions related to access to the boxes containing the documents.

(iii) Agencies will acknowledge receipt of referral notifications. They should notify the agency that placed the tabs that the review is complete. Any additional equities noted in the review must be annotated on the tab and brought to the attention of the agency that tabbed the document so the tabbing agency can notify those newly identified agencies.

(iv) Equity Notification Database. Agencies may also use an electronic notification database as a means of notification. Use of such a database, when available, will constitute referral and acknowledgement of referrals received under the Order.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for NATO and other foreign government information, agency heads or their designee(s) (hereinafter referred to as agency heads) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director, Information Security Oversight Office (ISOO), to facilitate that office's oversight responsibility. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasure benefits versus cost.

(c) NATO classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instructions I–69 and I–70. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at § 2001.53 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) An agency head who originates or handles classified information shall refer any matter pertaining to the implementation of this Directive that he or she cannot resolve to the Director, ISOO for resolution.

§ 2001.41 Responsibilities of holders [4.1].

Authorized persons who have access to classified information are responsible for:

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

§ 2001.42 Standards for security equipment [4.1].

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

§ 2001.43 Storage [4.1].

(a) *General.* Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) *Requirements for physical protection.* (1) Top Secret. Top Secret information shall be stored by one of the following methods:

(i) In a GSA-approved security container with one of the following supplemental controls:

(A) Continuous protection by cleared guard or duty personnel;

(B) Inspection of the security container every two hours by cleared guard or duty personnel;

(C) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation [Acceptability of Intrusion Detection Equipment (IDE): All IDE must be UL-listed (or equivalent as defined by the agency head) and approved by the agency head. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head.]; or

(D) Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L–2740.

(ii) An open storage area constructed in accordance with § 2001.43, which is equipped with an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not.

(iii) An IDS-equipped vault with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) Secret. Secret information shall be stored by one of the following methods:

(i) In the same manner as prescribed for Top Secret information;

(ii) In a GSA-approved security container or vault without supplemental controls; or

(iii) In either of the following:

(A) Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock; or

(B) An open storage area. In either case, one of the following supplemental controls is required:

(*1*) The location that houses the container or open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(*2*) Cleared guard or duty personnel shall inspect the security container or open storage area once every four hours; or

(*3*) An IDS (per paragraph (b)(1)(i)(C) of this section) with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation. [In addition to one of these supplemental controls specified in paragraphs (b)(2)(iii)(B)(*1*) through (*3*), security-in-depth as determined by the agency head is required as part of the supplemental controls for a non-GSA-approved container or open storage area storing Secret information.]

(3) Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

(c) *Combinations.* Use and maintenance of dial-type locks and other changeable combination locks.

(1) Equipment in service. The classification of the combination shall

be the same as the highest level of classified information that is protected by the lock. Combinations to dial-type locks shall be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(i) Whenever such equipment is placed into use;

(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(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 a standard combination.

(d) *Key operated locks.* When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established.

§ 2001.44 Information controls [4.1, 4.2].

(a) *General.* Agency heads shall establish a system of control measures which assure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(b) *Reproduction.* Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:

(1) Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

(2) Unless restricted by the originating Agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

(3) Copies of classified information shall be subject to the same controls as the original information; and

(4) The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

§ 2001.45 Transmission [4.1, 4.2].

(a) *General.* Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Directive.

(b) *Dispatch.* Agency heads shall establish procedures which ensure that:

(1) All classified information physically transmitted outside facilities shall be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible. Intended recipients shall be identified by name only as part of an attention line. The following exceptions apply:

(i) If the classified information is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

(ii) If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;

(iii) If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;

(iv) Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

(v) When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a high security padlock, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(c) *Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.*

(1) Top Secret. Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service.

(2) Secret. Secret information shall be transmitted by:

(i) Any of the methods established for Top Secret; U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature and Indemnity block, item 11–B, on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited; and

(ii) Agency heads may, on an exceptional basis and when an urgent requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the General Services Administration contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (39 CFR chapter I) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of classified information. The

sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

(3) Confidential. Confidential information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, when the recipient is a U.S. Government facility, the Confidential information may be transmitted via U.S. First Class Mail. However, Confidential information shall not be transmitted to government contractor facilities via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked to indicate that the information is not to be forwarded, but is to be returned to sender. The use of street-side mail collection boxes is prohibited.

(d) *Transmission methods to a U.S. Government facility located outside the U.S.* The transmission of classified information to a U.S. Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

(e) *Transmission of U.S. classified information to foreign governments.* Such transmission shall take place between designated government representatives using the transmission methods described in paragraph (d) of this section. When classified information is transferred to a foreign government or its representative a signed receipt is required.

(f) *Receipt of classified information.* Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. As noted in paragraph (e) of this section, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.

§ 2001.46 Destruction [4.1, 4.2].

(a) *General.* Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing.

(b) *Technical guidance.* Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media and processing equipment components may be obtained by submitting all pertinent information to the National Security Agency/Central Security Service, Directorate for Information Systems Security, Fort Meade, MD 20755. Specifications concerning appropriate equipment and standards for the destruction of other storage media may be obtained from the GSA.

§ 2001.47 Loss, possible compromise or unauthorized disclosure [4.1, 4.2].

(a) *General.* Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) *Cases involving information originated by a foreign government or another U.S. government agency.* Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) *Inquiry/investigation and corrective actions.* Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) *Department of Justice and legal counsel coordination.* Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with—

(1) The Department of Justice, and

(2) The legal counsel of the agency where the individual responsible is assigned or employed.

§ 2001.48 Special access programs [4.3].

(a) *General.* The safeguarding requirements of this Directive may be enhanced for information in Special Access Programs (SAP), established under the provisions of Section 4.3 of E.O. 12958, as amended, by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) *Significant interagency support requirements.* Agency heads must ensure that a Memorandum of Agreement/Understanding (MOA/MOU) is established for each Special Access Program that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

§ 2001.49 Telecommunications automated information systems and network security [4.1, 4.2].

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Index of National Security Telecommunications and Information Systems Security Issuances (NSTISSI) and Director of Central Intelligence Directive (DCID) 6/3.

§ 2001.50 Technical security [4.1].

Based upon the risk management factors referenced in § 2001.40 of this directive agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures (TSCM) and TEMPEST necessary to detect or deter exploitation of classified

information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, entitled Tempest Countermeasures for Facilities, and SPB Issuance 6–97, entitled National Policy on Technical Surveillance Countermeasures.

§ 2001.51 Emergency authority [4.2].

(a) Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding and destruction of classified information during certain emergency situations.

(b) In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

(1) Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

(2) Limit the number of individuals who receive it;

(3) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in subpart C of this directive, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

(i) A description of the disclosed information;

(ii) To whom the information was disclosed;

(iii) How the information was disclosed and transmitted;

(iv) Reason for the emergency release;

(v) How the information is being safeguarded; and

(vi) A description of the briefings provided and a copy of the nondisclosure agreements signed.

§ 2001.52 Open storage areas [4.1].

This section describes the construction standards for open storage areas.

(a) *Construction.* The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.

(b) *Doors.* Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three-position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.

(c) *Vents, ducts, and miscellaneous openings.* All vents, ducts, and similar openings in excess of 96 square inches (and over 6 inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system.

(d) *Windows.*

(1) All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

(2) Windows at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area.)

§ 2001.53 Foreign Government Information [4.1].

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I–69 and I–70. To the extent practical, and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government, hereafter ''originating government.''

(a) *Top Secret.* Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

(b) *Secret.* Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

(c) *Confidential.* Records need not be maintained for foreign government Confidential information unless required by the originator.

(d) *Restricted and other foreign government information provided in confidence.* In order to assure the protection of other foreign government information provided in confidence (*e.g.*, foreign government ''Restricted,'' ''Designated,'' or unclassified provided in confidence), such information must be classified under E.O. 12958 as amended. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the following requirements shall be met:

(1) Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be marked, ''This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).'' The notation, ''Modified Handling Authorized,'' may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

(2) Documents shall be provided only to those who have an established need-to-know, and where access is required by official duties;

(3) Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

(4) Documents shall be stored in such a manner so as to prevent unauthorized access;

(5) Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

(e) Third-country transfers. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

Subpart E—Self-Inspections

§ 2001.60 General [5.4].

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the agency's classified product. ''Self-inspection'' means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under the Order.

(b) *Applicability.* These standards are binding on all executive branch agencies that create or handle classified information. Pursuant to Executive Order 12829, the National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions and safeguards applicable to industry, including the conduct of contractor self-inspections. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958, as amended and this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* The official(s) responsible for the program shall determine the means and methods for the conduct of self-inspections. These may include:

(1) A review of relevant security directives, guides and instructions;

(2) Interviews with producers and users of classified information;

(3) A review of access and control records and procedures; and

(4) A review of a sample of classified documents generated by agency activities.

(e) *Frequency.* The official(s) responsible for the program shall set the frequency of self-inspections on the basis of program needs and the degree of classification activity. Activities that generate significant amounts of classified information should conduct at least one document review per year.

(f) *Reporting.* The format for documenting findings shall be set by the official(s) responsible for the program.

§ 2001.61 Coverage [5.4(d)(4)].

(a) *General.* These standards are not all-inclusive. Each agency may expand upon the coverage according to program and policy needs. Each self-inspection of an agency activity need not include all the elements covered in this section. Agencies without original classification authority need not include in their self-inspections those elements of coverage pertaining to original classification.

(b) *Elements of coverage.*

(1) Original classification.

(i) Evaluate original classification authority's general understanding of the process of original classification, including the:

(A) Applicable standards for classification;

(B) Levels of classification and the damage criteria associated with each; and

(C) Required classification markings.

(ii) Determine if delegations of original classification authority conform with the requirements of the Order, including whether:

(A) Delegations are limited to the minimum required to administer the program;

(B) Designated original classification authorities have a demonstrable and continuing need to exercise this authority;

(C) Delegations are in writing and identify the official by name or position title; and

(D) New requests for delegation of classification authority are justified.

(iii) Assess original classification authority's familiarity with the duration of classification requirements, including:

(A) Assigning a specific date or event for declassification that is less than 10 years when possible;

(B) Establishing ordinarily a 10 year duration of classification when an earlier date or event cannot be determined; and

(C) Limiting extensions of classification for specific information not to exceed 25 years for permanently valuable records or providing a 25 year exemption.

(iv) Conduct a review of a sample of classified information generated by the inspected activity to determine the propriety of classification and the application of proper and full markings.

(v) Evaluate classifiers' actions to comply with the standards specified in § 2001.15 and § 2001.32 of this part, relating to classification and declassification guides, respectively.

(vi) Verify observance with the prohibitions on classification and limitations on reclassification.

(vii)Assess whether the agency's classification challenges program meets the requirements of the Order and this part.

(2) Derivative classification. Assess the general familiarity of individuals who classify derivatively with the:

(i) Conditions for derivative classification;

(ii) Requirement to consult with the originator of the information when questions concerning classification arise;

(iii) Proper use of classification guides; and

(iv) Proper and complete application of classification markings to derivatively classified documents.

(3) Declassification.

(i) Verify whether the agency has established, to the extent practical, a system of records management to facilitate public release of declassified documents.

(ii) Evaluate the status of the agency declassification program, including the requirement to:

(A) Comply with the automatic declassification provisions regarding historically valuable records over 25 years old;

(B) Declassify, when possible, historically valuable records prior to accession into the National Archives;

(C) Provide the Archivist with adequate and current declassification guides;

(D) Ascertain that the agency's mandatory review program conforms to established requirements; and

(E) Determine whether responsible agency officials are cooperating with the ISOO Director to coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(4) Safeguarding.

(i) Monitor agency adherence to established safeguarding standards.

(ii) 5.4(c) of the Order—Verify whether the agency has established to the extent practical a records system designed and maintained to optimize the safeguarding of classified information.

(iii) Assess compliance with controls for access to classified information.

(iv) Evaluate the effectiveness of the agency's program in detecting and processing security violations and preventing recurrences.

(v) Assess compliance with the procedures for identifying, reporting and processing unauthorized disclosures of classified information.

(vi) Evaluate the effectiveness of procedures to ensure that:

(A) The originating agency exercises control over the classified information it generates;

(B) Holders of classified information do not disclose information originated by another agency without that agency's authorization; and

(C) Departing or transferred officials return all classified information in their possession to authorized agency personnel.

(5) Security education and training. Evaluate the effectiveness of the agency's security education and training program in familiarizing appropriate personnel with classification procedures; and determine whether the program meets the standards specified in subpart F of this part.

(6) Management and oversight.

(i) Determine whether original classifiers have received prescribed training.

(ii) Verify whether the agency's special access programs:

(A) Adhere to specified criteria in the creation of these programs;

(B) Are kept to a minimum;

(C) Provide for the conduct of internal oversight; and

(D) Include an annual review of each program to determine whether it continues to meet the requirements of the Order.

(iii) Assess whether:

(A) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(B) Producers and users of classified information receive guidance with respect to security responsibilities and requirements;

(C) Controls to prevent unauthorized access to classified information are effective;

(D) Contingency plans are in place for safeguarding classified information used in or near hostile areas;

(E) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: Original classifiers; security managers; classification management officers; and security specialists; and other employees whose duties significantly involve the creation or handling of classified information; and

(F) A method is in place for collecting information on the costs associated with the implementation of the Order.

Subpart F—Security Education and Training

§ 2001.70 General [5.4].

(a) *Purpose.* This subpart sets standards for agency security education and training programs. Implementation of these standards should:

(1) Ensure that all executive branch employees who create, process or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

(2) Increase uniformity in the conduct of agency security education and training programs; and

(3) Reduce improper classification, safeguarding and declassification practices.

(b) *Applicability.* These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirements, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958, as amended and of this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods. Agencies shall maintain records about the programs it has offered and employee participation in them.

(e) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

§ 2001.71 Coverage [5.4(d)(3)].

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classification authorities, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this part according to the agency's program and policy needs.

(b) *Elements of initial coverage.* All cleared agency personnel shall receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. Such training must be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information. The following areas should be considered for inclusion in initial briefings.

(1) Roles and responsibilities.

(i) What are the responsibilities of the senior agency official, classification management officers, the security manager and the security specialist?

(ii) What are the responsibilities of agency employees who create or handle classified information?

(iii) Who should be contacted in case of questions or concerns about classification matters?

(2) Elements of classifying and declassifying information.

(i) What is classified information and why is it important to protect it?

(ii) What are the levels of classified information and the damage criteria associated with each level?

(iii) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(iv) What are the general requirements for declassifying information?

(v) What are the procedures for challenging the classification status of information?

(3) Elements of safeguarding.

(i) What are the proper procedures for safeguarding classified information?

(ii) What constitutes an unauthorized disclosure and what are the criminal, civil, and administrative penalties associated with these disclosures?

(iii) What are the general conditions and restrictions for access to classified information?

(iv) What should an individual do when he or she believes safeguarding standards may have been violated?

(c) *Specialized security education and training.* Original classification authorities, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) Original Classification Authorities.

(i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

(iii) What are the standards that a designated classifier must meet to classify information?

(iv) What discretion does the Original Classification Authority have in classifying information, for example, foreign government information.

(v) What is the process for determining duration of classification?

(vi) What are the prohibitions and limitations on classifying information?

(vii) What are the basic markings that must appear on classified information?

(viii) What are the general standards and procedures for declassification?

(2) Declassification authorities other than original classification authorities.

(i) What are the standards, methods and procedures for declassifying information under Executive Order 12958, as amended?

(ii) What are the standards for creating and using agency declassification guides?

(iii) What is contained in the agency's automatic declassification plan?

(iv) What are the agency responsibilities for the maintenance of a declassification database?

(3) Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the creation or handling of classified information.

(i) What are the original and derivative classification processes and the standards applicable to each?

(ii) What are the proper and complete classification markings, as described in subpart B of this part?

(iii) What are the authorities, methods and processes for downgrading and declassifying information?

(iv) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(v) What are the requirements for creating and updating classification and declassification guides?

(vi) What are the requirements for controlling access to classified information?

(vii) What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(viii) What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

(ix) What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(x) What are the requirements for oversight of the security classification program, including agency self-inspections?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: The continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) Practices applicable to U.S. officials traveling overseas;

(2) Procedures for protecting classified information processed and stored in automated information systems;

(3) Methods for dealing with uncleared personnel who work in proximity to classified information;

(4) Responsibilities of personnel serving as couriers of classified information; and

(5) Security requirements that govern participation in international programs.

Subpart G—Reporting and Definitions

§ 2001.80 Statistical reporting [5.2(b)(4)].

Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§ 2001.81 Accounting for costs [5.4(d)(8)].

(a) Information on the costs associated with the implementation of the Order will be collected from the agencies. The agencies will provide data to ISOO on the cost estimates for classification-related activities. ISOO will report these cost estimates annually to the President. The agency senior official should work

closely with the agency comptroller to ensure that the best estimates are collected.

(b) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under Executive Order 12829, and consistent with agreements entered into under section 202 of E.O. 12829, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will report these cost estimates annually to the President.

§ 2001.82 Definitions [6.1].

(a) *''Accessioned Records''* means records of permanent historical value in the legal custody of NARA.

(b) *''Authorized person''* means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

(c) *''Cleared commercial carrier''* means a carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

(d) *''Control''* means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(e) *''Declassified or Declassification''* means the authorized change in the status of information from classified information to unclassified information.

(f) *''Equity''* means information originally classified by or under the control of an agency.

(g) *''Exempted''* means nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under E.O. 12958, as amended.

(h) *''Federal Record''* includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference, and stocks of publications and processed documents are not included. (44 U.S.C. 3301)

(i) *''File series''* means a body of related records created or maintained by an agency, activity, office or individual. The records may be related by subject, topic, form, function, or filing scheme. An agency, activity, office, or individual may create or maintain several different file series, each serving a different function. Examples may include a subject file, alphabetical name index, chronological file, or a record set of agency publications. File series frequently correspond to items on a NARA-approved agency records schedule. Some very large series may contain several identifiable sub-series, and it may be appropriate to treat sub-series as discrete series for the purposes of the Order.

(j) *''Newly Discovered Records''* means records that were inadvertently not reviewed prior to the effective date of automatic declassification because the agency declassification authority was unaware of their existence.

(k) *''Open storage area''* means an area constructed in accordance with section 2001.62 and authorized by the agency head for open storage of classified information.

(l) *''Pass/Fail (P/F)''* means a declassification technique that regards information at the full document or folder level. Any exemptible portion of a document or folder may result in exemption (failure) of the entire documents or folders. Documents or folders that contain no exemptible information are passed and therefore declassified. Documents within exempt folders are exempt from automatic declassification. Declassified documents may be subject to FOIA exemptions other than the security exemption ((b)(1)), and the requirements placed by legal authorities governing Presidential records and materials.

(m) *''Permanent Records''* means any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973.

(n) *''Presidential Historical Materials and Records''* means the papers or records of the former Presidents under the legal control of the Archivist pursuant to sections 2107, 2111, 2111note, or 2203 of title 44, U.S.C., as defined at 44 U.S.C. 2111, 2111note, and 2001.

(o) *''Records''* means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(p) *''Redaction''* means the removal of exempted information from copies of a document.

(q) *''Security-in-depth''* means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during non-working hours.

(r) *''Tab''* means a narrow paper sleeve placed around a document or group of documents in such a way that it would be readily visible.

(s) *''Transferred Records''* means records transferred to agency storage facilities or a federal records center.

(t) *''Temporary Records''* means federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called disposable records.

(u) *''Unscheduled Records''* means federal records whose final disposition has not been approved by NARA. All records that fall under a NARA approved records control schedule are considered to be scheduled records.

(v) *''Vault''* means an area approved by the agency head which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry. A modular vault approved by the General Services Administration (GSA) may be used in lieu of a vault as prescribed in the first sentence of this paragraph (e). Vaults shall be equipped with a GSA-approved vault door and lock.

§ 2001.83 Effective date [6.3].

Part 2001 shall become effective September 22, 2003.

PART 2004—DIRECTIVE ON SAFEGUARDING CLASSIFIED NATIONAL SECURITY INFORMATION [Removed and reserved.]

■ 2. Remove and reserve 32 CFR part 2004.

Dated: September 15, 2003.

J. William Leonard,

Director, Information Security Oversight Office.

[FR Doc. 03–24047 Filed 9–18–03; 12:01 pm]

BILLING CODE 7515–01–P