Federal Register

Monday,
June 28, 2010

Part V

National Archives and Records Administration

Information Security Oversight Office

32 CFR Parts 2001 and 2003
Classified National Security Information; Final Rule

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Parts 2001 and 2003

[FDMS Docket ISOO–10–0001]

RIN 3095–AB63

Classified National Security Information

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

ACTION: Implementing directive; final rule.

SUMMARY: The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), is publishing this Directive as a final rule and pursuant to Executive Order 13526 (hereafter the Order), 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.

DATES: *Effective Date:* June 25, 2010.

FOR FURTHER INFORMATION CONTACT: William J. Bosanko, Director, Information Security Oversight Office, at 202–357–5250.

SUPPLEMENTARY INFORMATION: This final rule is issued pursuant to the provisions of 5.1(a) and (b) of Executive Order 13526, issued December 29, 2009, and published January 5, 2010 (75 FR 707), and amends 32 CFR part 2001 published on September 22, 2003 (68 FR 55168). 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. The Archivist of the United States (the Archivist) 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 13526, which was issued on December 29, 2009. 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, as amended. Moreover, since Executive Order 13526 becomes effective on June 27, 2010, 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.

Regulatory Impact

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 in 32 CFR Parts 2001 and 2003

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, Standard Forms.

■ For the reasons set forth in the preamble, the Information Security Oversight Office, NARA, is amending 32 CFR Chapter XX as follows:

■ 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—Scope of Part

Sec.

Subpart B—Classification

Subpart C—Identification and Markings

Subpart D—Declassification

Subpart E—Safeguarding

Subpart F—Self-Inspections

Subpart G—Security Education and Training

Subpart H—Standard Forms

Subpart I—Reporting and Definitions

Authority: Sections 5.1(a) and (b), E.O. 13526, (75 FR 707, January 5, 2010).

Subpart A—Scope of Part

§ 2001.1 Purpose and scope.

(a) This part is issued under Executive Order. (E.O.) 13526, *Classified National Security Information* (the Order). Section 5 of the Order provides that the Director of the Information Security Oversight Office (ISOO) shall develop and issue such directives as are necessary to implement the Order.

(b) The Order provides that these directives are binding on agencies. Section 6.1(a) of the Order defines "agency" to mean any "Executive agency" as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) For the convenience of the user, the following table provides references between the sections contained in this part and the relevant sections of the Order.

CFR section	Related section of E.O. 13526
2001.10 Classification standards	1.1, 1.4
2001.11 Original classification authority	1.3
2001.12 Duration of classification	1.5
2001.13 Classification prohibitions and limitations	1.7
2001.14 Classification challenges	1.8
2001.15 Classification guides	2.2
2001.16 Fundamental classification guidance review	1.9
2001.20 General	1.6
2001.21 Original classification	1.6(a)
2001.22 Derivative classification	2.1
2001.23 Classification marking in the electronic environment	1.6
2001.24 Additional requirements	1.6
2001.25 Declassification markings	1.5, 1.6, 3.3
2001.26 Automatic declassification exemption markings	3.3
2001.30 Automatic declassification	3.3, 3.7
2001.31 Systematic declassification review	3.4
2001.32 Declassification guides	3.3, 3.7
2001.33 Mandatory review for declassification	3.5, 3.6
2001.34 Referrals	3.3, 3.6, 3.7
2001.35 Discretionary declassification	3.1
2001.36 Classified information in the custody of private organizations or individuals	none
2001.37 Assistance to the Department of State	none
2001.40 General	4.1
2001.41 Responsibilities of holders	4.1
2001.42 Standards for security equipment	4.1
2001.43 Storage	4.1
2001.44 Reciprocity of use and inspection of facilities	4.1
2001.45 Information controls	4.1, 4.2
2001.46 Transmission	4.1, 4.2
2001.47 Destruction	4.1, 4.2
2001.48 Loss, possible compromise, or unauthorized disclosure	4.1, 4.2
2001.49 Special access programs	4.3
2001.50 Telecommunications, automated information systems, and network security	4.1, 4.2
2001.51 Technical security	4.1
2001.52 Emergency authority	4.2
2001.53 Open storage areas	4.1
2001.54 Foreign government information	4.1
2001.55 Foreign disclosure of classified information	4.1(i)(2)
2001.60 Self-Inspections, General	5.4
2001.70 Security Education and Training, General	5.4
2001.71 Coverage	1.3(d), 2.1(d), 3.7(b), 4.1(b), 5.4(d)(3)
2001.80 Prescribed standard forms	5.2(b)(7)
2001.90 Agency annual reporting requirements	1.3(c), 5.2(b)(4), 5.4(d)(4), 5.4(d)(8)
2001.91 Other agency reporting requirements	1.3(d), 1.7(c)(3), 1.9(d), 2.1(d), 5.5
2001.92 Definitions	6.1

Subpart B—Classification

§ 2001.10 Classification standards.

Identifying or describing damage to the national security. Section 1.1(a) of the Order specifies the conditions that must be met when making classification decisions. Section 1.4 specifies that information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security. 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 pursuant to the Order or law.

§ 2001.11 Original classification authority.

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

(b) *Requests for original classification authority.* Agencies not possessing such authority shall forward requests to the Director of 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 National Security Advisor within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the procedures of this paragraph.

(c) *Reporting delegations of original classification authority.* All delegations of original classification authority shall be reported to the Director of ISOO. This can be accomplished by an initial submission followed by updates on a frequency determined by the senior agency official, but at least annually.

§ 2001.12 Duration of classification.

(a) *Determining duration of classification for information originally classified under the Order*—(1) *Establishing duration of classification.* Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an original classification authority shall follow the sequence listed in paragraphs (a)(1)(i), (ii), and (iii) of this section when determining the duration of classification for information originally classified under this Order.

(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) *Duration of classification of special categories of information.* The only exceptions to the sequence in paragraph (a)(1) of this section are as follows:

(i) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, the duration shall be up to 75 years and shall be designated with the following marking, "50X1–HUM;" or

(ii) If an original classification authority is classifying information that should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, the duration shall be up to 75 years and shall be designated with the following marking, "50X2–WMD."

(b) *Extending duration of classification for information 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.

(1) If the date or event assigned by the original classification authority has not passed, 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 origin of the record.

(2) If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may reclassify the information in accordance with the Order and this Directive only if it meets the standards for classification under sections 1.1 and 1.5 of the Order as well as section 3.3 of the Order, if appropriate.

(3) In all cases, 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.

(c) *Duration of 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. If the specific date or event has not passed, an original classification authority with jurisdiction over the information may extend the duration in accordance with the requirements of paragraph (b) of this section. If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may only reclassify information in accordance with the standards and procedures under the Order and this Directive. If the information is contained in records determined to be permanently valuable, and the prescribed date or event will take place more than 25 years from the date of origin of the document, the declassification of the information will instead be subject to section 3.3 of the Order.

(2) *Indefinite duration of classification.* For information marked with X1, X2, X3, X4, X5, X6, X7, or X8; "Originating Agency's Determination Required" or its acronym "OADR," "Manual Review" or its acronym "MR;" "DCI Only;" "DNI Only;" and any other marking indicating an indefinite duration of classification under a prior order; or in those cases where a document is missing a required declassification instruction or the instruction is not complete:

(i) A declassification authority, as defined in section 3.1(b) of the Order, may declassify it;

(ii) An original classification authority with jurisdiction over the information may re-mark the information to establish a duration of classification of no more than 25 years from the date of origin of the document, 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 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.

(3) *Release of imagery acquired by space-based intelligence reconnaissance systems.* The duration of classification of imagery as defined in E.O. 12951, *Release of Imagery Acquired by Space-Based Intelligence Reconnaissance Systems,* that is otherwise marked with an indefinite duration, such as "DCI Only" or "DNI Only," shall be established by the Director of National Intelligence in accordance with E.O. 12951 and consistent with E.O. 13526. Any such information shall be remarked in accordance with instructions prescribed by the Director of National Intelligence.

§ 2001.13 Classification prohibitions and limitations.

(a) *Declassification without proper authority.* Classified information that has been declassified without proper authority, as determined by an original classification authority with jurisdiction over the information, remains classified and administrative action shall be taken to restore markings and controls, as appropriate. All such determinations shall be reported to the senior agency official who shall promptly provide a written report to the Director of ISOO.

(1) If the information at issue is in records in the physical and legal custody of the National Archives and Records Administration (NARA) and has been made available to the public, the original classification authority with jurisdiction over the information shall, as part of determining whether the restoration of markings and controls is appropriate, consider whether the removal of the information from public purview will significantly mitigate the

harm to national security or otherwise draw undue attention to the information at issue. Written notification, classified when appropriate under the Order, shall be made to the Archivist, which shall include a description of the record(s) at issue, the elements of information that are classified, the duration of classification, and the specific authority for continued classification. If the information at issue is more than 25 years of age and the Archivist does not agree with the decision, the information shall nonetheless be temporarily withdrawn from public access and shall be referred to the Director of ISOO for resolution in collaboration with affected parties.

(b) *Reclassification after declassification and release to the public under proper authority.* In making the decision to reclassify information that has been declassified and released to the public under proper authority, the agency head must approve, in writing, a determination on a document-by-document basis that the reclassification is required to prevent significant and demonstrable damage to the national security. As part of making such a determination, the following shall apply:

(1) The information must be reasonably recoverable without bringing undue attention to the information which means that:

(i) Most individual recipients or holders are known and can be contacted and all instances of the information to be reclassified will not be more widely disseminated;

(ii) If the information has been made available to the public via a means such as Government archives or reading room, consideration is given to length of time the record has been available to the public, the extent to which the record has been accessed for research, and the extent to which the record and/or classified information at issue has been copied, referenced, or publicized; and

(iii) If the information has been made available to the public via electronic means such as the internet, consideration is given as to the number of times the information was accessed, the form of access, and whether the information at issue has been copied, referenced, or publicized.

(2) If the reclassification concerns a record in the physical custody of NARA and has been available for public use, reclassification requires notification to the Archivist and approval by the Director of ISOO.

(3) 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.

(4) The reclassified information must be appropriately marked in accordance with section 2001.24(l) and safeguarded. The markings should include the authority for and the date of the reclassification action.

(5) Once the reclassification action has occurred, it must be reported to the National Security Advisor and to the Director of ISOO by the agency head or senior agency official within 30 days. The notification must include details concerning paragraphs (b)(1) and (3) of this section.

(c) *Classification by compilation.* A determination that information is classified through the compilation of unclassified information is a derivative classification action based upon existing original classification guidance. If the compilation of unclassified information reveals a new aspect of information that meets the criteria for classification, it shall be referred to an original classification authority with jurisdiction over the information to make an original classification decision.

§ 2001.14 Classification challenges.

(a) *Challenging classification.* Authorized holders, including authorized holders outside the classifying agency, who want 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 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 (Panel) for a decision. The challenger may also forward the challenge to the Panel 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 Panel.

(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 this Directive. 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 and to ensure the integrity of the classification process.

§ 2001.15 Classification guides.

(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 and position, or personal identifier;

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

(9) Prescribe a specific date or event for declassification, the marking "50X1–HUM" or "50X2–WMD" as appropriate, or one or more of the exemption codes listed in 2001.26(a)(2), provided that:

(i) The exemption has been approved by the Panel under section 3.3(j) of the Order;

(ii) The Panel is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and

(iii) The exemption code is accompanied with a declassification date or event that has been approved by the Panel.

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

(d) *Reviewing and updating classification guides.* (1) Agencies shall incorporate original classification decisions into classification guides as soon as practicable.

(2) Originators of classification guides are encouraged to consult the users of guides and other subject matter experts 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.

§ 2001.16 Fundamental classification guidance review.

(a) *Performance of fundamental classification guidance reviews.* An initial fundamental classification guidance review shall be completed by every agency with original classification authority and which authors security classification guides no later than June 27, 2012. Agencies shall conduct fundamental classification guidance reviews on a periodic basis thereafter. The frequency of the reviews shall be determined by each agency considering factors such as the number of classification guides and the volume and type of information they cover. However, a review shall be conducted at least once every five years.

(b) *Coverage of reviews.* At a minimum, the fundamental classification guidance review shall focus on:

(1) Evaluation of content.

(i) Determining if the guidance conforms to current operational and technical circumstances; and

(ii) Determining if the guidance meets the standards for classification under section 1.4 of the Order and an assessment of likely damage under section 1.2 of the Order; and

(2) Evaluation of use:

(i) Determining if the dissemination and availability of the guidance is appropriate, timely, and effective; and

(ii) An examination of recent classification decisions that focuses on ensuring that classification decisions reflect the intent of the guidance as to what is classified, the appropriate level, the duration, and associated markings.

(c) *Participation in reviews.* The agency head or senior agency official shall direct the conduct of a fundamental classification guidance review and shall ensure the appropriate agency subject matter experts participate to obtain the broadest possible range of perspectives. To the extent practicable, input should also be obtained from external subject matter experts and external users of the reviewing agency's classification guidance and decisions.

(d) *Reports on results.* Agency heads shall provide a detailed report summarizing the results of each classification guidance review to ISOO and release an unclassified version to the public except when the existence of the guide or program is itself classified.

Subpart C—Identification and Markings

§ 2001.20 General.

A uniform security classification system requires that standard markings or other indicia be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information 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.

(a) *Primary markings.* At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

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

Classified By: David Smith, Chief, Division 5

or

Classified By: ID#IMNO1

(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 on the "Reason" line 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 covert action), 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;

(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; or

(H) The development, production, or use of 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: 1.4(g)

(4) *Declassification instructions.* The duration of the original classification decision shall be placed on the "Declassify On" line. When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD. Events must be reasonably definite and foreseeable. The original classification authority will apply one of the following instructions:

(i) A date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which is equal to or less than 10 years from the date of the original decision. The duration of classification would be marked as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20201014 or
Declassify On: Completion of Operation

(ii) 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, 2010, apply a date up to 25 years on the "Declassify On" line:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20351010

(iii) If the classified information should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, no date or event is required and the marking "50X1–HUM" shall be used in the "Declassify On" line; or

(iv) If the classified information should clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, no date or event is required and the marking "50X2–WMD" shall be used in the "Declassify On" line.

(b) *Overall marking.* The highest level of classification is determined by the highest level of any one portion within the document and 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, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies.

(1) To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, and "(C)" for Confidential will be used.

(2) Portions which do not meet the standards of the Order for classification shall be marked with "(U)" for Unclassified.

(3) In cases where portions are segmented such as paragraphs, sub-paragraphs, bullets, and sub-bullets and the classification level is the same throughout, it is sufficient to put only one portion marking at the beginning of the main paragraph or main bullet. If there are different levels of classification among these segments, then all segments shall be portion marked separately in order to avoid over-classification of any one segment. If the information contained in a sub-paragraph or sub-bullet is a higher level of classification than its parent paragraph or parent bullet, this does not make the parent paragraph or parent bullet classified at that same level. Each portion shall reflect the classification level of that individual portion and not any other portions. At the same time, any portion, no matter what its status, is still capable of determining the overall classification of the document.

(d) *Dissemination control and handling markings.* Many agencies require additional control and handling markings that supplement the overall classification markings. See § 2001.24(j) for specific guidance.

(e) *Date of origin of document.* The date of origin of the document shall be indicated in a manner that is immediately apparent.

§ 2001.22 Derivative classification.

(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) *Identity of persons who apply derivative classification markings.* Derivative classifiers shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document. 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: Peggy Jones, Lead Analyst, Research and Analysis Division or
Classified By: ID # IMN01

(c) *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, 2008, Office of Administration, Department of Good Works or
Derived From: CG No. 1, Department of Good Works, dated October 20, 2008

(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 include a listing of the source materials on, or attached to, each 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, 2009, Department of Good Works, Office of Administration

(d) *Reason for classification.* The reason for the original classification decision, as reflected in the source document(s) or classification guide, is

not transferred in a derivative classification action.

(e) *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, unless it contains one of the declassification instructions as listed in paragraph (e)(3) of this section. If the source document is missing the declassification instruction, then a calculated date of 25 years from the date of the source document (if available) or the current date (if the source document date is not available) shall be carried forward by the derivative classifier.

(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.

(3) When a document is classified derivatively either from a source document(s) or a classification guide that contains one of the following declassification instructions, "Originating Agency's Determination Required," "OADR," or "Manual Review," "MR," or any of the exemption markings X1, X2, X3, X4, X5, X6, X7, and X8, the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document's date or event to be placed in the "Declassify On" line.

(i) If a document is marked with the declassification instructions "DCI Only" or "DNI Only" and does not contain information described in E.O. 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document's date or event to be placed in the "Declassify On" line.

(ii) If a document is marked with "DCI Only" or "DNI Only" and the information is subject to E.O. 12951, the derivative classifier shall use a date or event as prescribed by the Director of National Intelligence.

(4) When determining the most restrictive declassification instruction among multiple source documents, adhere to the following hierarchy for determining the declassification instructions for the "Declassify On" line:

(i) 50X1–HUM or 50X2–WMD, or an ISOO-approved designator reflecting the Panel approval for classification beyond 50 years in accordance with section 3.3(h)(2) of the Order;

(ii) 25X1 through 25X9, with a date or event;

(iii) A specific declassification date or event within 25 years;

(iv) Absent guidance from an original classification authority with jurisdiction over the information, a calculated 25-year date from the date of the source document.

(5) When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD.

(f) *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).

(g) *Portion marking.* Each portion of a derivatively classified document shall be marked immediately preceding the portion to which it applies, in accordance with its source, and as provided in § 2001.21(c).

(h) *Dissemination control and handling markings.* Many agencies require additional control and handling markings that supplement the overall classification markings. See § 2001.24(j) for specific guidance.

(i) *Date of origin of document.* The date of origin of the document shall be indicated in a manner that is immediately apparent.

§ 2001.23 Classification marking in the electronic environment.

(a) *General.* Classified national security information in the electronic environment shall be:

(1) Subject to all requirements of the Order.

(2) Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, "Classified By," "Derived From," "Reason" for classification (originally classified information only), and "Declassify On."

(3) Marked with proper classification markings when appearing in an electronic output (*e.g.,* database query) in which users of the information will need to be alerted to the classification status of the information.

(4) Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the original classification authority. In cases where classified information in an electronic environment cannot be marked in this manner, a warning shall be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information.

(5) Prohibited from use as source of derivative classification if it is dynamic in nature (*e.g.,* wikis and blogs) and where information is not marked in accordance with the Order.

(b) *Markings on classified e-mail messages.* (1) E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the e-mail shall reflect the classification of the header and body of the message. This includes the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail. A single linear text string showing the overall classification and markings shall be included in the first line of text and at the end of the body of the message after the signature block.

(2) Classified e-mail shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (*i.e.,* link) to another document shall be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.

(3) A classified signature block shall be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.

(4) Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(5) For a classified e-mail, the classification authority block shall be placed after the signature block, but before the overall classification marking string at the end of the e-mail. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) When forwarding or replying to an e-mail, individuals shall ensure that, in addition to the markings required for the content of the reply or forward e-mail itself, the markings shall reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(c) *Marking Web pages with classified content.* (1) Web pages shall be classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of information to which the web materials link shall also be marked based on its own content.

(2) The overall classification marking string for every web page shall reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation is utilized, a text equivalent of the overall classification marking string shall be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified Web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

(5) Classified Web pages shall include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides shall carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure shall be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

(d) *Marking classified URLs.* URLs provide unique addresses in the electronic environment for web content and shall be portion marked based on the classification of the content of the URL itself. The URL shall not be portion marked to reflect the classification of the content to which it points. URLs shall be developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark shall be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL. An example may appear as:

http://www.center.xyz/SECRET/filename_(S).html
http://www.center.xyz/filename2_(TS).html
http://www.center.xyz/filename_(TS//NF).html

(e) *Marking classified dynamic documents and relational databases.* (1) A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.

(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings shall be applied to and displayed on the document. If such a mechanism does not exist, the default should be the highest level of information in the database and a warning shall be applied at the top of each page of the document. Such content shall not be used as a basis for derivative classification. An example of such an applied warning may appear as:

> This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification; refer instead to the pertinent classification guide(s).

(3) This will alert the users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users shall be encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as classification guides and points of contact shall be established to assist with these inquiries.

(4) Users developing a document based on query results from a database must properly mark the document in accordance with § 2001.22. If there is doubt about the correct markings, users should contact the database originating agency for guidance.

(f) *Marking classified bulletin board postings and blogs.* (1) A blog, an abbreviation of the term "web log," is a Web site consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.

(2) The overall classification marking string for every bulletin board or blog shall reflect the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.

(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) The overall classification marking string for the bulletin board posting, blog entry, or comment shall reflect the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings shall be entered manually or utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.

(5) Bulletin board postings, blog entries, or comments shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(g) *Marking classified wikis.* (1) Initial wiki submissions shall include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. Systems shall provide a means to log the identity of each user, the changes made, and the time and date of each change.

(3) Wiki articles and entries shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

(h) *Instant messaging, chat, and chat rooms.* (1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string shall also appear.

(2) Chat rooms shall display system-high overall classification markings and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall

classification marking, and a classification authority block.

(i) *Attached files.* When files are attached to another electronic message or document, the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with § 2001.24(b).

(ii) *Reserved.*

§ 2001.24 Additional requirements.

(a) *Marking prohibitions.* Markings other than "Top Secret," "Secret," and "Confidential" shall not be used to identify classified national security information.

(b) *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)

(c) *Foreign government information.* Unless otherwise evident, documents that contain foreign government information should include the marking, "This Document Contains (indicate country of origin) Information." Agencies may also require that the portions of the documents that contain the foreign government information 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. 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. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information.

(d) *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.

(e) *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.

(f) *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, created, 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.

(g) *Classification by compilation/aggregation.* Compilation of items that are individually unclassified may be classified if the compiled information meets the standards established in section 1.2 of the Order and reveals an additional association or relationship, as determined by the original classification authority. Any unclassified portions will be portion marked (U), while the overall markings will reflect the classification of the compiled information even if all the portions are marked (U). In any such situation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified compilation, and when they do not.

(h) *Commingling of Restricted Data (RD) and Formerly Restricted Data (FRD) with information classified under the Order.* (1) To the extent practicable, the commingling in the same document of RD or FRD with information classified under the Order should be avoided. When it is not practicable to avoid such commingling, the marking requirements in the Order and this Directive, as well as the marking requirements in 10 CFR part 1045, *Nuclear Classification and Declassification,* must be followed.

(2) Automatic declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from the automatic declassification provisions of the Order until the RD or FRD designation is properly removed by the Department of Energy. When the Department of Energy determines that an RD or FRD designation may be removed, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.

(3) For commingled documents, the "Declassify On" line required by the Order and this Directive shall not include a declassification date or event and shall instead be annotated with "Not Applicable (or N/A) to RD/FRD portions" and "See source list for NSI portions." The source list, as described in § 2001.22(c)(1)(ii), shall include the declassification instruction for each of the source documents classified under the Order and shall not appear on the front page of the document.

(4) If an RD or FRD portion is extracted for use in a new document, the requirements of 10 CFR part 1045 must be followed.

(5) If a portion classified under the Order is extracted for use in a new document, the requirements of the Order and this Directive must be followed. The declassification date for the extracted portion shall be determined by using the source list required by § 2001.22(c)(1)(ii), the pertinent classification guide, or consultation with the original classification authority with jurisdiction for the information. However, if a commingled document is not portion marked, it shall not be used as a source for a derivatively classified document.

(6) If a commingled document is not portion marked based on appropriate authority, annotating the source list with the declassification instructions and including the "Declassify on" line in accordance with paragraph (h)(3) of this section are not required. The lack of declassification instructions does not eliminate the requirement to process commingled documents for declassification in accordance with the Order, this Directive, the Atomic Energy

Act, or 10 CFR part 1045 when they are requested under statute or the Order.

(i) *Transclassified Foreign Nuclear Information (TFNI).* (1) As permitted under 42 U.S.C. 2162(e), the Department of Energy shall remove from the Restricted Data category such information concerning the atomic energy programs of other nations as the Secretary of Energy and the Director of National Intelligence jointly determine to be necessary to carry out the provisions of 50 U.S.C. 403 and 403–1 and safeguarded under applicable Executive orders as "National Security Information" under a process called transclassification.

(2) When Restricted Data information is transclassified and is safeguarded as "National Security Information," it shall be handled, protected, and classified in conformity with the provisions of the Order and this Directive. Such information shall be labeled as "TFNI" and with any additional identifiers prescribed by the Department of Energy. The label "TFNI" shall be included on documents to indicate the information's transclassification from the Restricted Data category and its declassification process governed by the Secretary of Energy under the Atomic Energy Act.

(3) Automatic declassification of documents containing TFNI is prohibited. Documents marked as containing TFNI are excluded from the automatic declassification provisions of the Order until the TFNI designation is properly removed by the Department of Energy. When the Department of Energy determines that a TFNI designation may be removed, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.

(j) *Approved dissemination control and handling markings.* (1) Dissemination control and handling markings identify the expansion or limitation on the distribution of the information. These markings are in addition to, and separate from, the level of classification.

(2) Only those external dissemination control and handling markings approved by ISOO or, with respect to the Intelligence Community by the Director of National Intelligence for intelligence and intelligence-related information, may be used by agencies to control and handle the dissemination of classified information pursuant to agency regulations and to policy directives and guidelines issued under section 5.4(d)(2) and section 6.2(b) of the Order. Such approved markings shall be uniform and binding on all agencies and must be available in a central registry.

(3) If used, the dissemination control and handling markings will appear at the top and bottom of each page after the level of classification.

(k) *Portion marking waivers.* (1) 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. The request must also demonstrate that the requested waiver will not create impediments to information sharing. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

(2) Any approved portion marking waiver will be temporary with specific expiration dates.

(3) Requests for portion marking waivers from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director of National Intelligence or his or her designee. Requests for portion marking waivers from elements of the Department of Defense (to include pertinent elements of the Intelligence Community) should include a statement of support from the Secretary of Defense or his or her designee. Requests for portion marking waivers from elements of the Department of Homeland Security should include a statement of support from the Secretary of Homeland Security or his or her designee.

(4) A document not portion marked, based on an ISOO-approved waiver, must contain a warning statement that it may not be used as a source for derivative classification.

(5) If a classified document that is not portion marked, based on an ISOO-approved waiver, is transmitted outside the originating organization, the document must be portion marked unless otherwise explicitly provided in the waiver approval.

(l) *Marking information that has been reclassified.* Specific information may only be reclassified if all the conditions of section 1.7(d) of the Order and its implementing directives have been met.

(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 and position, or by personal identifier of the original classification authority;

(iii) Declassification instructions;

(iv) A concise reason for classification, including reference to the applicable classification category from section 1.4 of the Order; and

(v) The date the reclassification action was taken.

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

(m) *Marking of electronic storage media.* Classified computer media such as USB sticks, hard drives, CD ROMs, and diskettes shall be marked to indicate the highest overall classification of the information contained within the media.

§ 2001.25 Declassification markings.

(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, 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 identity of the declassification authority, by name and position, or by personal identifier, or the title and date of the declassification guide. If the identity of the declassification authority must be protected, a personal identifier may be used or the information may be retained in agency files.

(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, 2008

§ 2001.26 Automatic declassification exemption markings.

(a) *Marking information exempted from automatic declassification at 25 years.* (1) When the Panel has approved an agency proposal to exempt permanently valuable information from automatic declassification at 25 years, the "Declassify On" line shall be revised to include the symbol "25X" plus the

number(s) that corresponds to the category(ies) in section 3.3(b) of the Order. Except for when the exemption pertains to information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, or a human intelligence source, or key design concepts of weapons of mass destruction, the revised "Declassify On" line shall also include the new date for declassification as approved by the Panel, not to exceed 50 years from the date of origin of the record. Records that contain information, the release of which should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, are exempt from automatic declassification at 50 years.

(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, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

25X2: reveal information that would assist in the development, production, 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 formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

25X6: reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

25X7: reveal information that would 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 impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

25X9: violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

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

Declassify On: 25X4, 20501001

(4) Documents should not be marked with a "25X" marking until the agency has been informed that the Panel concurs with the proposed exemption.

(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 and may only apply such a marking as approved by the Panel under section 3.3(j) of the Order.

(6) Information containing foreign government information will be marked with a date in the "Declassify On" line that is no more than 25 years from the date of the document unless the originating agency has applied for and received Panel approval to exempt foreign government information from declassification at 25 years. Upon receipt of Panel approval, the agency may use either the 25X6 or 25X9 exemption markings, as appropriate, in the "Declassify On" followed by a date that has also been approved by the Panel. An example might appear as: 25X6, 20600129, or 25X9, 20600627. The marking "subject to treaty or international agreement" is not to be used at any time.

(b) *Marking information exempted from automatic declassification at 50 years.* Records exempted from automatic declassification at 50 years shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within five years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(1) When the information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source, the marking shall be "50X1–HUM."

(2) When the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction, the marking shall be "50X2–WMD."

(3) In extraordinary cases in which the Panel has approved an exemption from declassification at 50 years under section 3.3(h) of the Order, the same procedures as those under § 2001.26(a) will be followed with the exception that the number "50" will be used in place of the "25."

(4) Requests for exemption from automatic declassification at 50 years from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director of National Intelligence or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Defense (to include pertinent elements of the Intelligence community) should include a statement of support from the Secretary of Defense or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Homeland Security should include a statement of support from the Secretary of the Department of Homeland Security or his or her designee.

(c) *Marking information exempted from automatic declassification at 75 years.* Records exempted from automatic declassification at 75 years shall be automatically declassified on December 31 of the year that has been formally approved by the Panel.

(1) Information approved by the Panel as exempt from automatic declassification at 75 years shall be marked "75X" with the appropriate automatic declassification exemption category number followed by the approved declassification date or event.

(2) Requests for exemption from automatic declassification at 75 years from elements of the Intelligence Community (to include pertinent elements of the Department of Defense) should include a statement of support from the Director of National Intelligence or his or her designee. Requests for automatic declassification exemptions from elements of the Department of Defense (to include pertinent elements of the Intelligence community) should include a statement of support from the Secretary of Defense or his or her designee.

Subpart D—Declassification

§ 2001.30 Automatic declassification.

(a) *General.* All departments and agencies that have original classification authority or previously had original classification authority, or maintain records determined to be permanently valuable that contain classified national security information, 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.

(b) *Presidential papers, materials, and records.* The Archivist shall establish procedures for the declassification of presidential, vice-presidential, or White House materials transferred to the legal

custody of NARA or maintained in the presidential libraries.

(c) *Classified information in the custody of contractors, licensees, certificate holders, or grantees.* Pursuant to the provisions of the 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 the Order. Until such a determination has been made by an appropriate agency official, such records shall not be subject to automatic declassification, or destroyed, 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, 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 agency in possession shall serve as the originating agency and shall be responsible for actions for those records in accordance with section 3.3 of the Order and in consultation with the Director of the National Declassification Center (NDC).

(f) *Processing records originated by another agency.* When an agency uncovers classified records originated by another agency that appear to meet the criteria for referral according to section 3.3(d) of the Order, the finding agency shall identify those records for referral to the originating agency as described in § 2001.34.

(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 become 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 become 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 at 25 years.

(h) *Temporary records and non-record materials.* Classified information contained in records determined not to be permanently valuable or non-record materials shall be processed in accordance with section 3.6(c) of the Order.

(i) *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 does not permit automatic or unilateral declassification. 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 prior to declassification.

(j) *Assistance to the Archivist of the United States.* Agencies shall consult with the Director of the NDC established in section 3.7 of the Order concerning their automatic declassification programs. At the request of the Archivist, agencies shall cooperate with the Director of the NDC in developing priorities for the declassification of records to ensure that declassification is accomplished efficiently and in a timely manner. Agencies shall consult with NARA and the Director of the NDC 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 and sufficient information about agency declassification actions, including metadata and other processing information, when records are accessioned by NARA. This data shall include certification by the agency that the records have been reviewed in accordance with Public Law 105–261, section 3161 governing Restricted Data and Formerly Restricted Data.

(k) *Use of approved declassification guides.* Approved declassification guides are the sole basis for the exemption from automatic declassification of specific information as provided in section 3.3(b) of the Order and the sole basis for the continued classification of information under section 3.3(h) of the Order. These guides must be prepared in accordance with section 3.3(j) of the Order and include additional pertinent detail relating to the exemptions described in sections 3.3(b) and 3.3(h) of the Order, and follow the format required of declassification guides as described in § 2001.32. During a review under section 3.3 of the Order, it is expected that agencies will use these guides to identify specific information for exemption from automatic declassification. It is further expected that the guides or detailed declassification guidance will be made available to the NDC under section 3.7(b) of the Order and to appropriately cleared individuals of other agencies to support equity recognition.

(l) *Automatic declassification date.* No later than December 31 of the year that is 25 years from the date of origin, classified records determined to be permanently valuable shall be automatically declassified unless automatic declassification has been delayed for any reason as provided in § 2001.30(n) and sections 3.3(b) and (c) of the Order. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(m) *Exemption from Automatic Declassification at 25, 50, or 75 years.* Agencies may propose to exempt from automatic declassification specific information, either by reference to information in specific records, in specific file series of records, or in the form of a declassification guide, in accordance with section 3.3(j) of the Order. Agencies may propose to exempt information within five years of, but not later than one year 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 Panel, of the specific information being proposed for exemption from automatic declassification.

(n) *Delays in the onset of automatic declassification*—(1) *Media that make a review for possible declassification exemptions more difficult or costly.* An agency head or senior agency official shall consult with the Director of the NDC before delaying automatic declassification for up to five years for classified information contained in media that make a review for possible declassification more difficult or costly. When determined by NARA or jointly determined by NARA and another agency, the following may be delayed

due to the increased difficulty and cost of conducting declassification processing:

(i) Records requiring extraordinary preservation or conservation treatment, to include reformatting, to preclude damage to the records by declassification processing;

(ii) Records which pose a potential menace to health, life, or property due to contamination by a hazardous substance; and

(iii) Electronic media if the media is subject to issues of software or hardware obsolescence or degraded data.

(2) *Referred records.* Records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies and could reasonably be expected to fall under one or more of the exemption categories of section 3.3(b) of the Order shall be identified prior to the onset of automatic declassification for later referral to those agencies. Declassification reviewers shall be trained periodically on other agency equities to aid in the proper identification of other agency equities eligible for referral.

(i) Information properly identified as a referral to another agency contained in records accessioned by NARA or in the custody of the presidential libraries shall be subject to automatic declassification only after the referral has been made available by NARA for agency review in accordance with § 2001.34, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of the Order.

(ii) Information properly identified as a referral to another agency contained in records maintained in the physical, but not legal, custody of NARA shall be subject to automatic declassification after accessioning and in accordance with § 2001.34, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of the Order.

(3) *Newly discovered records.* An agency head or senior agency official must consult with the Director of ISOO on any decision to delay automatic declassification of newly discovered records no later than 90 days, from the discovery of the records. The notification shall identify the records, their volume, the anticipated date for declassification, and the circumstances of the discovery. An agency may be granted up to three years from the date of discovery to make a declassification, exemption, or referral determination. If referrals to other agencies are properly identified, they will be handled in accordance with subparagraphs 2(i) and 2(ii) above.

(4) *Integral file blocks.* Classified records within an integral file block that are otherwise subject to automatic declassification under section 3.3 of the Order shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block. For purposes of automatic declassification, integral file blocks shall contain only records dated within ten years of the oldest record in the file block. Integral file blocks applied prior to December 29, 2009, that cover more than ten years remain in effect until December 31, 2012, unless an agency requests an extension from the Director of ISOO on a case-by-case basis prior to December 31, 2011, which is subsequently approved.

(5) *File series exemptions.* Agencies seeking to delay the automatic declassification of a specific series of records as defined in section 6.1(r) of the Order because it almost invariably contains information that falls within one or more of the exemption categories under section 3.3(b) must submit their request in accordance with section 3.3(c) of the Order to the Director of ISOO, serving as Executive Secretary of the Panel, at least one year prior to the onset of automatic declassification. Once approved by the Panel, the records in the file series exemption remain subject to section 3.5 of the Order. This delay applies only to records within the specific file series. Copies of records within the specific file series or records of a similar topic to the specific file series located elsewhere may be exempted in accordance with exemptions approved by the Panel.

(o) *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. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

(p) *Restricted Data and Formerly Restricted Data.* (1) Restricted Data and Formerly Restricted Data 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 under the Atomic Energy Act of 1954, as amended, 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 or identified as potentially containing unmarked Restricted Data or Formerly Restricted Data shall be referred to the Department of Energy in accordance with § 2001.34(b)(8).

(4) Automatic declassification of documents containing Restricted Data or Formerly Restricted Data is prohibited. Documents marked as containing Restricted Data or Formerly Restricted Data are excluded from the automatic declassification provisions of the Order until the Restricted Data or Formerly Restricted Data designation is properly removed by the Department of Energy. When the Department of Energy determines that a Restricted Data or Formerly Restricted Data designation may be removed, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification provisions of the Order and this Directive.

(5) Any document containing information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, shall be referred to the Department of Energy.

(6) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out the provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, information concerning foreign nuclear programs (*e.g.,* intelligence assessments or reports, foreign nuclear program information provided to the U.S. Government) shall be declassified when comparable information concerning the United States nuclear program is declassified. When the Secretary of Energy determines that information concerning foreign nuclear programs may be declassified, any remaining information classified under the Order must be referred to the appropriate agency in accordance with the declassification

provisions of the Order and this Directive.

§ 2001.31 Systematic declassification review.

(a) *General.* Agencies shall establish systematic review programs for those records containing information exempted from automatic declassification. This includes individual records as well as file series of records. Agencies shall prioritize their review of such records in accordance with priorities established by the NDC.

§ 2001.32 Declassification guides.

(a) *Preparation of declassification guides.* Beginning one year after the effective date of this directive, declassification guides must be submitted to the Director of ISOO, serving as the Executive Secretary of the Panel, at least one year prior to the onset of automatic declassification for approval by the Panel. Currently approved guides remain in effect until a new guide is approved, to the extent they are otherwise applied consistent with section 3.3(b) of the Order. The information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions must be based upon specific content and not type of document. Exemptions for general categories of information are not acceptable. Agencies must prepare guides that clearly delineate between the exemptions proposed under sections 3.3(b), 3.3(h)(1) and (2), and 3.3(h)(3).

(b) *General content of declassification guides.* Declassification guides must be specific and detailed as to the information requiring continued classification and clearly and demonstrably explain the reasons for continued classification. Declassification guides shall:

(1) Be submitted by the agency head or the designated senior agency official;

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

(3) State precisely the information that the agency proposes to exempt from automatic declassification and to specifically declassify;

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

(5) 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), and, if appropriate, section 3.3(h) of the Order; and

(ii) A date or event for declassification that is in accordance with section 3.3(b) or section 3.3(h).

(c) *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.

(d) *Dissemination of guides.* (1) Declassification guides shall be disseminated within the agency to be used by all personnel with declassification review responsibilities.

(2) Declassification guides or detailed declassification guidance shall be submitted to the Director of the NDC in accordance with section 3.7(b)(3) of the Order.

§ 2001.33 Mandatory review for declassification.

(a) *U.S. originated information*—(1) *Regulations.* Each agency shall publish, and update as needed or required, in the **Federal Register** regulations concerning the handling of mandatory declassification review requests, to include the identity of the person(s) or office(s) to which requests should be addressed.

(2) *Processing*—(i) *Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request must be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests may be denied by agencies for processing under this section. In responding to mandatory declassification review requests, agencies shall 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 laws, those declassified portions of the requested information that constitute a coherent segment. Upon denial, in whole or in part, of an initial request, the agency shall also notify the requestor of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial. Agencies receiving mandatory review requests are expected to conduct a line-by-line review of the record(s) for public access and are expected to release the information to the requestor, unless that information is prohibited from release under the provisions of a statutory authority, such as, but not limited to, the Freedom of Information Act, (5 U.S.C. 552), as amended, the Presidential Records Act of 1978 (44 U.S.C. 2201–2207), or the National Security Act of 1947 (Pub. L. 235, 61 Stat. 496, 50 U.S.C. Chapter 15).

(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 promptly process the request for declassification and release in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency. The referring agency is responsible for collecting all agency review results and informing the requestor of any final decision regarding the declassification of the requested information unless a prior arrangement has been made with the originating 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 requestor in writing of the final determination and of the reasons for any denial. The appellate authority must inform the requestor of his or her final appeal rights to the Panel.

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

(v) *Records subject to mandatory declassification review.* Records containing information exempted from automatic declassification in accordance with section 3.3(c) of the Order or with § 2001.30(n)(1) are still subject to the mandatory declassification review provisions of section 3.5 of the Order.

(b) *Foreign government information.* Except as provided in this paragraph, agencies 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 does not permit automatic or unilateral declassification. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

(c) *Cryptologic information.* Mandatory declassification review requests for cryptologic information shall be processed in accordance with special procedures issued by the Secretary of Defense and, when cryptologic information pertains to intelligence activities, the Director of National Intelligence.

(d) *Intelligence information.* Mandatory declassification review requests for information pertaining to intelligence sources, methods, and activities shall be processed in accordance with special procedures issued by the Director of National Intelligence.

(e) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with 31 U.S.C. 9701 or relevant fee provisions in other applicable statutes.

(f) *Requests filed under mandatory declassification review and the Freedom of Information Act.* When a requester submits a request both under mandatory declassification review and the Freedom of Information Act (FOIA), the agency shall require the requestor to select one process or the other. If the requestor fails to select one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory declassification 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 (5 U.S.C. 552a), as amended, 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. The specific reason for the redaction, as provided for in section 1.4 or 3.3(b) of the Order, as applicable, must be included for each redaction. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

(i) *Limitations on requests.* Requests for mandatory declassification review made to an element of the Intelligence Community by anyone other than a citizen of the United States or an alien lawfully admitted for permanent residence, may be denied by the receiving Intelligence Community element. Documents required to be submitted for pre-publication review or other administrative process pursuant to an approved nondisclosure agreement are not subject to mandatory declassification review.

§ 2001.34 Referrals.

(a) *General.* Referrals are required under sections 3.3(d)(3) and 3.6(b) of the Order in order to ensure the timely, efficient, and effective processing of reviews and requests and in order to protect classified information from inadvertent disclosure.

(b) *Automatic declassification.* The referral process for records subject to automatic declassification entails identification of records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies. Those records that could reasonably be expected to fall under one or more of the exemptions in section 3.3(b) of the Order are eligible for referral. The referral process also entails formal notification to those agencies, making the records available for review by those agencies, and recording final agency determinations.

(1) In accordance with section 3.3(d)(3) of the Order, the identification of records eligible for referral is the responsibility of the primary reviewing agency and shall be completed prior to the date of automatic declassification established by section 3.3(a) of the Order.

(2) Except as otherwise determined by the Director of the NDC, primary reviewing agencies shall utilize the Standard Form 715, *Government Declassification Review Tab,* to tab and identify any Federal record requiring referral and record the referral in a manner that provides the referral information in an NDC database system.

(3) Notification of referral of records accessioned into NARA or in the custody of the presidential libraries, and making the records available for review, is the responsibility of NARA and shall be accomplished through the NDC.

(4) Within 180 days of the effective date of this provision, the NDC shall develop and provide the affected agencies with a comprehensive and prioritized schedule for the resolution of referrals contained in accessioned Federal records and Presidential records. The schedule shall be developed in consultation with the affected agencies, consider the public interest in the records, and be in accordance with the authorized delays to automatic declassification set forth in section 3.3(d) of the Order. The initial schedule shall cover the balance of the first effective fiscal year and four subsequent fiscal years. Thereafter, the schedule shall cover five fiscal years. The NDC shall consult with the affected agencies and update and provide such schedules annually.

(5) The NDC shall provide formal notification of the availability of a referral to the receiving agency and records will be subject to automatic declassification in accordance with the schedule promulgated by the NDC in paragraph (b)(4) of this section, unless the information has been properly exempted by an equity holding agency under section 3.3 of the Order.

(6) Records in the physical but not legal custody of NARA shall be subject to automatic declassification after accessioning and in accordance with paragraphs (b)(3) and (b)(5) of this section.

(7) Agencies that establish a centralized facility as described in section 3.7(e) may make direct referrals provided such activities fall within the priorities and schedule established by the NDC and the activity is otherwise coordinated with the NDC. In such cases, the centralized facility is responsible for providing formal notification of a referral to receiving agencies and for making the records available for review or direct formal referral to agencies by providing a copy of the records unless another mechanism is identified in coordination with the NDC. As established in section 3.3(d)(3)(B), referrals to agencies from a centralized agency records facility as described in section 3.7(e) of the Order will be automatically declassified up to three years after the formal notification has been made, if the receiving agency fails to provide a final determination.

(8) Records marked as containing Restricted Data or Formerly Restricted Data or identified as potentially

containing unmarked Restricted Data or Formerly Restricted Data shall be referred to the Department of Energy through the NDC. If the Department of Energy confirms that the document contains Restricted Data or Formerly Restricted Data, it shall then be excluded from the automatic declassification provisions of the Order until the Restricted Data or Formerly Restricted Data designation is properly removed.

(i) When the Department of Energy provides notification that a Restricted Data or Formerly Restricted Data designation is not appropriate or when it is properly removed, the record shall be processed for automatic declassification through the NDC.

(ii) In all cases, should the record be the subject of an access demand made pursuant to the Order or provision of law, the information classified pursuant to Executive order (rather than the Atomic Energy Act, as amended) must stand on its own merits.

(9) The NDC, as well as any centralized agency facility established under section 3.7(e) of the Order, shall track and document referral actions and decisions in a manner that facilitates archival processing for public access. Central agency facilities must work with the NDC to ensure documentation meets NDC requirements, and transfer all documentation on pending referral actions and referral decisions to the NDC when transferring the records to NARA.

(10) In all cases, receiving agencies shall acknowledge receipt of formal referral notifications in a timely manner. If a disagreement arises concerning referral notifications, the Director of ISOO will determine the automatic declassification date and notify the senior agency official, as well as the NDC or the primary reviewing agency.

(11) *Remote Archives Capture (RAC).* Presidential records or materials scanned in the RAC process shall be prioritized and scheduled for review by the NDC. The initial notification shall be made to the agency with primary equity, which shall have up to one year to act on its information and to identify all other equities eligible for referral. All such additional referrals in an individual record shall be made at the same time, and once notified by the NDC of an eligible referral, such receiving agencies shall have up to one year to review the records before the onset of automatic declassification.

(c) *Agencies eligible to receive referrals.* The Director of ISOO will publish annually a list of those agencies eligible to receive referrals for each calendar year.

(d) *Systematic declassification review.* The identification of equities shall be accomplished in accordance with paragraph (b) of this section. Priorities for review will be established by the NDC.

(e) *Identification of interests other than national security.* Referrals under sections 3.3(d)(3) and 3.6(b) of the Order shall be assumed to be intended for later public release unless withholding is otherwise authorized and warranted under applicable law. If a receiving agency proposes to withhold any such information, it must notify the referring agency at the time they otherwise respond to the referral. Such notification shall identify the specific information at issue and the pertinent law.

§ 2001.35 Discretionary declassification.

(a) In accordance with section 3.1(d) of the Order, agencies may declassify information when the public interest in disclosure outweighs the need for continued classification.

(b) Agencies may also establish a discretionary declassification program that is separate from their automatic, systematic, and mandatory review programs.

§ 2001.36 Classified information in the custody of private organizations or individuals.

(a) *Authorized holders.* Agencies may allow for the holding of classified information by a private organization or individual provided that all access and safeguarding requirements of the Order have been met. Agencies must provide declassification assistance to such organizations or individuals.

(b) *Others.* Anyone who becomes aware of organizations or individuals who possess potentially classified national security information outside of government control must contact the Director of ISOO for guidance and assistance. The Director of ISOO, in consultation with other agencies, as appropriate, will ensure that the safeguarding and declassification requirements of the Order are met.

§ 2001.37 Assistance to the Department of State.

Heads of agencies shall 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. If an agency fails to provide a final declassification review determination regarding a Department of State referral within 120 days of the date of the referral, or if applicable, within 120 days of the date of a High Level Panel decision, the Department of State, consistent with 22 U.S.C. 4353 and any implementing agency procedures, may seek the assistance of the Panel.

Subpart E—Safeguarding

§ 2001.40 General.

(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 foreign government information, agency heads or their designee(s) 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 of ISOO. 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) North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instruction (USSAN) 1–07. 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 § 2001.54 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) *Need-to-know determinations.* (1) Agency heads, through their designees, shall identify organizational missions

and personnel requiring access to classified information to perform or assist in authorized governmental functions. These mission and personnel requirements are determined by the functions of an agency or the roles and responsibilities of personnel in the course of their official duties. Personnel determinations shall be consistent with section 4.1(a) of the Order.

(2) In instances where the provisions of section 4.1(a) of the Order are met, but there is a countervailing need to restrict the information, disagreements that cannot be resolved shall be referred by agency heads or designees to either the Director of ISOO or, with respect to the Intelligence Community, the Director of National Intelligence, as appropriate. Disagreements concerning information protected under section 4.3 of the Order shall instead be referred to the appropriate official named in section 4.3 of the Order.

§ 2001.41 Responsibilities of holders.

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.

(a) *Storage.* The Administrator of the General Services Administration (GSA) shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications, qualified product lists or databases, and supply schedules for security equipment designed to provide secure storage for classified information. Whenever new secure storage equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of the GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

(b) *Destruction.* Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy classified information using any method covered by an EPL. However, equipment approved for use prior to January 1, 2011, and not found on an EPL, may be utilized for the destruction of classified information until December 31, 2016. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of classified information up to six years from the date of its removal from an EPL. In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction in accordance with this section. The Administrator of the GSA shall, to the maximum extent possible, coordinate supply schedules and otherwise seek to make equipment on an EPL available through the Federal Supply System.

§ 2001.43 Storage.

(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 in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53. In addition, supplemental controls are required as follows:

(i) For GSA-approved containers, one of the following supplemental controls:

(A) Inspection of the container every two hours by an employee cleared at least to the Secret level;

(B) 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 in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head; or

(C) Security-In-Depth coverage of the area in which the container is located, provided the container is equipped with a lock meeting Federal Specification FF–L–2740.

(ii) For open storage areas covered by Security-In-Depth, an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(iii) For open storage areas not covered by Security-In-Depth, personnel responding to the alarm shall arrive within five minutes of the alarm annunciation.

(2) *Secret.* Secret information shall be stored in the same manner as Top Secret information or, 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. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:

(i) Inspection of the container or open storage area every four hours by an employee cleared at least to the Secret level; or

(ii) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

(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.* Combinations to dial-type locks shall be changed only by persons 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 combination lock should be reset to a standard combination of 50–25–50 for built-in combination locks or 10–20–30 for combination padlocks.

(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 included in implementing regulations required under section 5.4(d)(2) of the Order.

(e) *Repairs.* The neutralization and repair of GSA-approved security containers and vault doors will be in accordance with FED STD 809.

§ 2001.44 Reciprocity of use and inspection of facilities.

(a) Once a facility is authorized, approved, certified, or accredited for classified use, then all agencies desiring to conduct classified work in the designated space(s) at the same security level shall accept the authorization, approval, certification, or accreditation without change, enhancements, or upgrades provided that no waiver, exception, or deviation has been issued or approved. In the event that a waiver exception, or deviation was granted in the original accreditation of the designated space(s), an agency seeking to utilize the designated facility space may require that a risk mitigation strategy be implemented or agreed upon prior to using the space(s).

(b) Subsequent security inspections or reviews for authorization, approval, certification, or accreditation purposes shall normally be conducted no more frequently than annually unless otherwise required due to a change in the designated facility space(s) or due to a change in the use or ownership of the facility space(s). This does not imply a formal one-year inspection or review requirement or establish any other formal period for inspections or review.

§ 2001.45 Information controls.

(a) *General.* Agency heads shall establish a system of control measures which assure that access to classified information is provided 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.

(1) *Combinations.* Combinations to locks used to secure vaults, open storage areas, and security containers that are approved for the safeguarding of classified information shall be protected in the same manner as the highest level of classified information that the vault, open storage area, or security container is used to protect.

(2) *Computer and information system passwords.* Passwords shall be protected in the same manner as the highest level of classified information that the computer or system is certified and accredited to process. Passwords shall be changed on a frequency determined to be sufficient to meet the level of risk assessed by the agency.

(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.

(c) *Forms.* The use of standard forms prescribed in Subpart H of this part is mandatory for all agencies that create and/or handle national security information.

(d) *Redaction*—(1) *Policies and procedures.* Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted. Agencies shall establish policies and procedures for the redaction of classified information from documents intended for release. Such policies and procedures require the approval of the agency head and shall be sufficiently detailed to ensure that redaction is performed consistently and reliably, using only approved redaction methods that permanently remove the classified information from copies of the documents intended for release. Agencies shall ensure that personnel who perform redaction fully understand the policies, procedures, and methods and are aware of the vulnerabilities surrounding the process.

(2) *Technical guidance for redaction.* Technical guidance concerning appropriate methods, equipment, and standards for the redaction of classified electronic and optical media shall be issued by NSA.

§ 2001.46 Transmission.

(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 combination padlock meeting Federal Specification FF–P–110, 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 or any other cleared or uncleared commercial carrier.

(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 block 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, when a requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the GSA 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 streetside 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 government-to-government transmission methods described in paragraph (d) of this section or through channels agreed to by the National Security Authorities of the two governments. 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.

§ 2001.47 Destruction.

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. Agencies shall comply with the destruction equipment standard stated in § 2001.42(b) of this Directive.

§ 2001.48 Loss, possible compromise or unauthorized disclosure.

(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 U.S. 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) *Reports to ISOO.* In accordance with section 5.5(e)(2) of the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:

(1) Is reported to oversight committees in the Legislative branch;

(2) May attract significant public attention;

(3) Involves large amounts of classified information; or

(4) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(e) *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.

§ 2001.49 Special access programs.

(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 the Order 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 is established for each SAP that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

§ 2001.50 Telecommunications automated information systems and network security.

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 Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation.*

§ 2001.51 Technical security.

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 and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, *TEMPEST Countermeasures for Facilities,* and SPB Issuance 6–97, *National Policy on Technical Surveillance Countermeasures.*

§ 2001.52 Emergency authority.

(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 § 2001.46, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified and 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.

(7) Information disclosed in emergency situations shall not be required to be declassified as a result of such disclosure or subsequent use by a recipient.

§ 2001.53 Open storage areas.

This section describes the minimum 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 within 18 feet of the ground 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).

§ 2001.54 Foreign government information.

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 USSAN 1–07. 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 in paragraphs (a) through (e) of this section 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 the Order. 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 persons in accordance with sections 4.1(a) and (h) of the Order;

(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.

§ 2001.55 Foreign disclosure of classified information.

Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government or international organization of governments, or any element thereof, in accordance with statute, the Order, directives implementing the Order, direction of the President, or with the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information. Markings used to implement this section shall be approved in accordance with § 2001.24(j). With respect to the Intelligence Community, the Director of National Intelligence may issue policy directives or guidelines pursuant to section 6.2(b) of the Order that modify such prior authorization.

Subpart F—Self-Inspections

§ 2001.60 General.

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include regular reviews of representative samples of the agency's original and derivative classification actions.

(b) *Responsibility.* The senior agency official is responsible for directing and administering the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility. The program shall be structured to provide the senior agency official with information necessary to assess the effectiveness of the classified national security information program within individual agency activities and the agency as a whole, in order to enable the senior agency official to fulfill his or her responsibility to oversee the agency's program under section 5.4(d) of the Order.

(c) *Approach.* The senior agency official shall determine the means and methods for the conduct of self-inspections.

(1) Self-inspections should evaluate the adherence to the principles and requirements of the Order and this directive and the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

(2) Regular reviews of representative samples of the agency's original and derivative classification actions shall encompass all agency activities that generate classified information. They shall include a sample of varying types of classified information (in document and electronic format such as e-mail) to provide a representative sample of the activity's classification actions. The sample shall be proportionally sufficient to enable a credible assessment of the agency's classified product. Agency personnel who are assigned to conduct reviews of agencies' original and derivative classification actions shall be knowledgeable of the classification and marking requirements of the Order and this directive, and have access to pertinent security classification guides. In accordance with section 5.4(d)(4) of the Order, the senior agency official shall authorize appropriate agency officials to correct misclassification actions.

(3) Self-inspections should include a review of relevant security directives and instructions, as well as interviews with producers and users of classified information.

(d) *Frequency.* Self-inspections shall be regular, ongoing, and conducted at least annually with the senior agency

official setting the frequency on the basis of program needs and the degree of classification activity. Activities that generate significant amounts of classified information shall include a representative sample of their original and derivative classification actions.

(e) *Coverage.* The senior agency official shall establish self-inspection coverage requirements based on program and policy needs. Agencies with special access programs shall evaluate those programs in accordance with sections 4.3(b)(2) and (4) of the Order, at least annually.

(f) *Reporting.* Agencies shall document the findings of self-inspections internally.

(1) *Internal.* The senior agency official shall set the format for documenting self-inspection findings. As part of corrective action for findings and other concerns of a systemic nature, refresher security education and training should address the underlying cause(s) of the issue.

(2) *External.* The senior agency official shall report annually to the Director of ISOO on the agency's self-inspection program. This report shall include:

(i) A description of the agency's self-inspection program to include activities assessed, program areas covered, and methodology utilized;

(ii) The assessment and a summary of the findings of the agency self-inspections in the following program areas: Original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight;

(iii) Specific information with regard to the findings of the annual review of the agency's original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies that were identified;

(iv) Actions that have been taken or are planned to correct identified deficiencies or misclassification actions, and to deter their reoccurrence; and

(v) Best practices that were identified during self-inspections.

Subpart G—Security Education and Training

§ 2001.70 General.

(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 of classification, safeguarding, and declassification policies and procedures;

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

(3) Reduce instances of over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices.

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

(c) *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, on-line presentations, and other media and methods. Each agency shall maintain records about the programs it has offered and employee participation in them.

(d) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program, subject to the following requirements:

(1) Initial training shall be provided to every person who has met the standards for access to classified information in accordance with section 4.1 of the Order.

(2) Original classification authorities shall receive training in proper classification and declassification prior to originally classifying information and at least once each calendar year thereafter.

(3) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the Order prior to derivatively classifying information and at least once every two years.

(4) Each agency shall provide some form of refresher security education and training at least annually for all its personnel who handle or generate classified information.

§ 2001.71 Coverage.

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial training, refresher training, specialized training, and termination briefings. This subpart establishes fundamental security education and training standards for original classification authorities, derivative classifiers, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. Agency officials responsible for the security education and training programs should determine the specific training to be provided according to the agency's program and policy needs.

(b) *Initial training.* 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 accessing classified information.

(c) *Training for original classification authorities.* Original classification authorities shall be provided detailed training on proper classification and declassification, with an emphasis on the avoidance of over-classification. At a minimum, the training shall cover classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(1) Personnel shall receive this training prior to originally classifying information.

(2) In addition to this initial training, original classification authorities shall receive training in proper classification and declassification at least once each calendar year.

(3) Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended until such training has taken place.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.

(ii) Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

(d) *Training for persons who apply derivative classification markings.* Persons who apply derivative classification markings shall receive

training in the proper application of the derivative classification principles of the Order, emphasizing the avoidance of over-classification. At a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(1) Personnel shall receive this training prior to derivatively classifying information.

(2) In addition to this preparatory training, derivative classifiers shall receive such training at least once every two years.

(3) Derivative classifiers who do not receive such mandatory training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training.

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers shall be documented.

(ii) Whenever such a waiver is granted, the individual shall receive the required training as soon as practicable.

(e) *Other specialized security education and training.* Classification management officers, security managers, security specialists, declassification authorities, and all other personnel whose duties significantly involve the creation or handling of classified information shall receive more detailed or additional training no later than six months after assumption of duties that require other specialized training.

(f) *Annual refresher security education and training.* Agencies shall provide annual refresher training to employees who create, process, or handle classified information. Annual refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Annual refresher training should also address identification and handling of other agency-originated information and foreign government information, as well as 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. Annual refresher training should also address issues or concerns identified during agency self-inspections.

(g) *Termination briefings.* Except in extraordinary circumstances, each agency shall ensure that each employee who is granted access to classified information and who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn or revoked 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.

(h) *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 H—Standard Forms

§ 2001.80 Prescribed standard forms.

(a) *General.* The purpose of the standard forms is to promote the implementation of the government-wide information security program. Standard forms are prescribed when their use will enhance the protection of national security information and/or will reduce the costs associated with its protection. The use of the standard forms prescribed is mandatory for agencies of the executive branch that create or handle national security information. As appropriate, these agencies may mandate the use of these forms by their contractors, licensees, or grantees who are authorized access to national security information.

(b) *Waivers.* Except for the SF 312, "Classified Information Nondisclosure Agreement," and the SF 714, "Financial Disclosure Report," (which are waiverable by the Director of National Intelligence, as the Security Executive Agent, under E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*) only the Director of ISOO may grant a waiver from the use of the prescribed standard forms. To apply for a waiver, an agency must submit its proposed alternative form to the Director of ISOO along with its justification for use. The Director of ISOO will review the request and notify the agency of the decision. Waivers approved prior to December 29, 2009, remain in effect and are subject to review.

(c) *Availability.* Agencies may obtain copies of the standard forms prescribed by ordering through FEDSTRIP/MILSTRIP or from the GSA Consumer Global Supply Centers, or the GSA Advantage on-line service. Some of these standard forms can be downloaded from the GSA Forms Library.

(d) *Standard Forms.* Standard forms required for application to national security information are as follows.

(1) *SF 311, Agency Security Classification Management Program Data:* The SF 311 is a data collection form completed by only those executive branch agencies that create and/or handle classified national security information. The form is a record of classification management data provided by the agencies. The agencies submit the completed forms on an annual basis to ISOO, no later than November 15 following the reporting period, for inclusion in a report to the President.

(2) *SF 312, Classified Information Nondisclosure Agreement:*

(i) The SF 312 is a nondisclosure agreement between the United States and an employee of the Federal Government or one of its contractors, licensees, or grantees. The prior execution of this form by an individual is necessary before the United States Government may grant that individual access to classified information, with the exception of an emergency as defined in section 4.2(b) of the Order.

(ii) Electronic signatures on SF–312s are prohibited.

(iii) The SF 312 is the current authorized form; if an employee originally signed the now outdated SF 189 or SF 189–A, or a form under an approved waiver, as agreement to nondisclosure, the forms remain valid. The SF 189 and SF 189–A are no longer available for use with new employees.

(iv) The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional at the discretion of the implementing agency. If an agency chooses not to record its debriefing by signing/dating the debriefing section of the SF 312, then

the agency shall provide an alternative record.

(v) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee, or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(vi) The provisions of the SF 312, the SF 189, and the SF 189–A do not supersede the provisions of 5 U.S.C. 2302, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(vii) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189–A in file systems from which an agreement can be expeditiously retrieved in the event that the United States must seek its enforcement or a subsequent employer must confirm its prior execution. The original, or a legally enforceable facsimile that is retained in lieu of the original, such as microfiche, microfilm, computer disk, or electronic storage medium, must be retained for 50 years following its date of execution. For agreements executed by civilian employees of the United States Government, an agency may store the executed copy of the SF 312 and SF 189 in the United States Office of Personnel Management's Official Personnel Folder as a long-term (right side) document for that employee. An agency may permit its contractors, licensees, and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractors, licensee, or grantee shall deliver the original or legally enforceable facsimile of the executed SF 312, SF 189, or SF 189–A of that employee to the Government agency primarily responsible for his or her classified work. A contractor, licensee, or grantee of an agency participating in the National Industrial Security Program shall provide the copy or legally enforceable facsimile of the executed SF 312, SF 189, or SF 189–A of a terminated employee to their cognizant security office. Each agency shall inform ISOO of the file systems that it uses to store these agreements for each category of affected individuals.

(viii) Only the Director of National Intelligence, as the Security Executive Agent, may grant an agency's request for a waiver from the use of the SF 312. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of the Special Security Center (SSC), Office of the Director of National Intelligence, along with a justification for its use. The Director, SSC, shall request a determination about the alternative agreement's enforceability from the Department of Justice.

(ix) The national stock number for the SF 312 is 7540–01–280–5499.

(3) *SF 700, Security Container Information:* The SF 700 provides the names, addresses, and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended. The form also includes the means to maintain a current record of the security container's combination and provides the envelope to be used to forward this information to the appropriate agency activity or official. If an agency determines, as part of its risk management strategy, that a security container information form is required, the SF 700 shall be used. Parts 2 and 2A of each completed copy of SF 700 shall be classified at the highest level of classification of the information authorized for storage in the security container. A new SF 700 must be completed each time the combination to the security container is changed. The national stock number for the SF 700 is 7540–01–214–5372.

(4) *SF 701, Activity Security Checklist:* The SF 701 provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability in the event that irregularities are discovered. If an agency determines, as part of its risk management strategy, that an activity security checklist is required, the SF 701 will be used. Completion, storage, and disposition of SF 701 will be in accordance with each agency's security regulations. The national stock number for the SF 701 is 7540–01–213–7899.

(5) *SF 702, Security Container Check Sheet:* The SF 702 provides a record of the names and times that persons have opened, closed, or checked a particular container that holds classified information. If an agency determines, as part of its risk management strategy, that a security container check sheet is required, the SF 702 will be used. Completion, storage, and disposal of the SF 702 will be in accordance with each agency's security regulations. The national stock number of the SF 702 is 7540–01–213–7900.

(6) *SF 703, TOP SECRET Cover Sheet:* The SF 703 serves as a shield to protect Top Secret classified information from inadvertent disclosure and to alert observers that Top Secret information is attached to it. If an agency determines, as part of its risk management strategy, that a TOP SECRET cover sheet is required, the SF 703 will be used. The SF 703 is affixed to the top of the Top Secret document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 703 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 703 is 7540–01–213–7901.

(7) *SF 704, SECRET Cover Sheet:* The SF 704 serves as a shield to protect Secret classified information from inadvertent disclosure and to alert observers that Secret information is attached to it. If an agency determines, as part of its risk management strategy, that a SECRET cover sheet is required, the SF 704 will be used. The SF 704 is affixed to the top of the Secret document and remains attached until the document is downgraded, requiring the appropriate classification level cover sheet, declassified, or destroyed. When the SF 704 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 704 is 7540–01–213–7902.

(8) *SF 705, CONFIDENTIAL Cover Sheet:* The SF 705 serves as a shield to protect Confidential classified information from inadvertent disclosure and to alert observers that Confidential information is attached to it. If an agency determines, as part of its risk management strategy, that a CONFIDENTIAL cover sheet is required, the SF 705 will be used. The SF 705 is affixed to the top of the Confidential document and remains attached until the document is destroyed. When the SF 705 has been appropriately removed, it may, depending upon its condition, be reused. The national stock number of the SF 704 is 7540–01–213–7903.

(9) *SF 706, TOP SECRET Label:* The SF 706 is used to identify and protect electronic media and other media that contain Top Secret information. The SF 706 is used instead of the SF 703 for media other than documents. If an agency determines, as part of its risk management strategy, that a TOP SECRET label is required, the SF 706 will be used. The SF 706 is affixed to the medium containing Top Secret

information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 706 is 7540–01–207–5536.

(10) *SF 707, SECRET Label:* The SF 707 is used to identify and protect electronic media and other media that contain Secret information. The SF 707 is used instead of the SF 704 for media other than documents. If an agency determines, as part of its risk management strategy, that a SECRET label is required, the SF 707 will be used. The SF 707 is affixed to the medium containing Secret information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 707 is 7540–01–207–5537.

(11) *SF 708, CONFIDENTIAL Label:* The SF 708 is used to identify and protect electronic media and other media that contain Confidential information. The SF 708 is used instead of the SF 705 for media other than documents. If an agency determines, as part of its risk management strategy, that a CONFIDENTIAL label is required, the SF 708 will be used. The SF 708 is affixed to the medium containing Confidential information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 708 is 7540–01–207–5538.

(12) *SF 709, CLASSIFIED Label:* The SF 709 is used to identify and protect electronic media and other media that contain classified information pending a determination by the classifier of the specific classification level of the information. If an agency determines, as part of its risk management strategy, that a CLASSIFIED label is required, the SF 709 will be used. The SF 709 is affixed to the medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. When a classifier has made a determination of the specific level of classification of the information contained on the medium, either the SF 706, SF 707, or SF 708 shall be affixed on top of the SF 709 so that only the SF 706, SF 707, or SF 708 is visible. The national stock number of the SF 709 is 7540–01–207–5540.

(13) *SF 710, UNCLASSIFIED Label:* In a mixed environment in which classified and unclassified information are being processed or stored, the SF 710 is used to identify electronic media and other media that contain unclassified information. Its function is to aid in distinguishing among those media that contain either classified or unclassified information in a mixed environment. If an agency determines, as part of its risk management strategy, that an UNCLASSIFIED label is required, the SF 710 will be used. The SF 710 is affixed to the medium containing unclassified information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. However, the label is small enough so that it can be wholly covered by a SF 706, SF 707, SF 708, or SF 709 if the medium subsequently contains classified information. The national stock number of the SF 710 is 7540–01–207–5539.

(14) *SF 711, DATA DESCRIPTOR Label:* The SF 711 is used to identify additional safeguarding controls that pertain to classified information that is stored or contained on electronic or other media. If an agency determines, as part of its risk management strategy, that a DATA DESCRIPTOR label is required, the SF 711 will be used. The SF 711 is affixed to the electronic medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. The SF 711 is ordinarily used in conjunction with the SF 706, SF 707, SF 708, or SF 709, as appropriate. Once the label has been applied, it cannot be removed. The SF 711 provides spaces for information that should be completed as required. The national stock number of the SF 711 is 7540–01–207–5541.

(15) *SF 714, Financial Disclosure Report:* When required by an agency head or by the Director of National Intelligence, as the Security Executive Agent, the SF 714 contains information that is used to make personnel security determinations, including whether to grant a security clearance; to allow access to classified information, sensitive areas, and equipment; or to permit assignment to sensitive national security positions. The data may later be used as a part of a review process to evaluate continued eligibility for access to classified information or as evidence in legal proceedings. The SF 714 assists law enforcement agencies in obtaining pertinent information in the preliminary stages of potential espionage and counter terrorism cases.

(16) *SF 715, Government Declassification Review Tab:* The SF 715 is used to record the status of classified national security information reviewed for declassification. The SF 715 shall be used in all situations that call for the use of a tab as part of the processing of records determined to be of permanent historical value. The national stock number for the SF 715 is 7540–01–537–4689.

Subpart I—Reporting and Definitions

§ 2001.90 Agency annual reporting requirements.

(a) *Delegations of original classification authority.* Agencies shall report delegations of original classification authority to ISOO annually in accordance with section 1.3(c) of the Order and § 2001.11(c).

(b) *Statistical reporting.* Each agency that creates or safeguards 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.

(c) *Accounting for costs.*

(1) 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.

(2) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O.12829, as amended, *National Industrial Security Program,* and consistent with agreements entered into under section 202 of E.O. 12989, as amended, 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.

(d) *Self-Inspections.* Agencies shall report annually to the Director of ISOO as required by section 5.4(d)(4) of the Order and outlined in § 2001.60(f).

§ 2001.91 Other agency reporting requirements.

(a) *Information declassified without proper authority.* Determinations that classified information has been declassified without proper authority shall be promptly reported in writing to the Director of ISOO in accordance with § 2001.13(a).

(b) *Reclassification actions.* Reclassification of information that has been declassified and released under

proper authority shall be reported promptly to the National Security Advisor and the Director of ISOO in accordance with section 1.7(c)(3) of the Order and § 2001.13(b).

(c) *Fundamental classification guidance review.* The initial fundamental guidance review is to be completed no later than June 27, 2012. Agency heads shall provide a detailed report summarizing the results of each classification guidance review to ISOO and release an unclassified version to the public in accordance with section 1.9 of the Order and § 2001.16(d).

(d) *Violations of the Order.* Agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under sections 5.5(b)(1), (2), or (3) of the Order and § 2001.48(d).

§ 2001.92 Definitions.

(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.

(c) *Classification management* means the life-cycle management of classified national security information from original classification to declassification.

(d) *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.

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

(f) *Employee* means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(g) *Equity* refers to information:

(1) Originally classified by or under the control of an agency;

(2) In the possession of the receiving agency in the event of transfer of function; or

(3) In the possession of a successor agency for an agency that has ceased to exist.

(h) *Exempted* means nomenclature and markings indicating information has been determined to fall within an enumerated exemption from automatic declassification under the Order.

(i) *Facility* means an activity of an agency authorized by appropriate authority to conduct classified operations or to perform classified work.

(j) *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)

(k) *Newly discovered records* means records that were inadvertently not reviewed prior to the effective date of automatic declassification because the appropriate agency personnel were unaware of their existence.

(l) *Open storage area* means an area constructed in accordance with § 2001.53 of this part and authorized by the agency head for open storage of classified information.

(m) *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 the Order.

(n) *Permanent records* means any Federal record that has been determined by the National Archives to have sufficient value to warrant its preservation in the National Archives. Permanent records include all records accessioned by the National Archives into the National Archives 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 the National Archives on or after May 14, 1973.

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

(1) Records that have been accessioned by the National Archives;

(2) Records that have been scheduled as permanent under a records disposition schedule approved by the National Archives; and

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

(p) *Presidential papers, historical materials, and records* means the papers or records of the former Presidents under the legal control of the Archivist pursuant to sections 2111, 2111 note, or 2203 of title 44, U.S.C.

(q) *Redaction* means the removal of classified information from copies of a document such that recovery of the information on the copy is not possible using any reasonably known technique or analysis.

(r) *Risk management principles* means the principles applied for assessing threats and vulnerabilities and implementing security countermeasures while maximizing the sharing of information to achieve an acceptable level of risk at an acceptable cost.

(s) *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 nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

(t) *Supplemental controls* means prescribed procedures or systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.

(u) *Temporary records* means Federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called *disposable records.*

(v) *Transclassification* means information that has been removed from

the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive orders as "National Security Information."

(w) *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.

PART 2003—[REMOVED]

■ 2. Under the authority of E.O. 12958, 60 FR 19825, 3 CFR Comp., p. 333 as amended by E.O. 13292, 68 FR 15315, March 28, 2003, remove and reserve 32 CFR part 2003.

Dated: June 22, 2010.

William J. Bosanko,

Director, Information Security Oversight Office.

Approved: June 22, 2010.

David S. Ferriero,

Archivist of the United States.

[FR Doc. 2010–15443 Filed 6–25–10; 8:45 am]

BILLING CODE 7515–01–P