§ 1909.18 Termination of access.

The Coordinator shall cancel any authorization whenever the Director of Personnel Security cancels the security clearance of a requester (or research associate, if any) or whenever the Agency Release Panel determines that continued access would not be in compliance with one or more of the requirements of 32 CFR 1909.14(a).
CHAPTER XX—INFORMATION SECURITY
OVERSIGHT OFFICE, NATIONAL ARCHIVES
AND RECORDS ADMINISTRATION

<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>Administrative procedures [Reserved]</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td>Classified national security information ....................</td>
<td>477</td>
</tr>
<tr>
<td>2002</td>
<td>General guidelines for systematic declassification review of foreign government information</td>
<td>502</td>
</tr>
<tr>
<td>2003</td>
<td>National security information—standard forms ....</td>
<td>507</td>
</tr>
<tr>
<td>2004</td>
<td>Directive on safeguarding classified national security information</td>
<td>514</td>
</tr>
</tbody>
</table>
PART 2000—ADMINISTRATIVE PROCEDURES [RESERVED]

PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION

Sec.
2001.10 Classification definitions and standards [1.1 and 1.2].
2001.11 Classification authority [1.4].
2001.12 Duration of classification [1.6].
2001.13 Classification challenges [1.9].
2001.14 Classification guides [2.3].

Subpart A—Classification

§ 2001.10 Classification definitions and standards [1.1 and 1.2].

(a) Definitions. (1) An original classification authority with jurisdiction over the information includes:
   (i) The official who authorized the original classification, if that official is still serving in the same position;
   (ii) The originator’s current successor in function;
   (iii) A supervisory official of either;
   (iv) The senior agency official under Executive Order 12958 (“the Order”).

(b) Permanently valuable information or permanent historical value refers to information contained in:
   (i) Records that have been accessioned into the National Archives of the United States;
   (ii) Records that have been scheduled as permanent under a records retention schedule approved by the National Archives and Records Administration (NARA); and
   (iii) Presidential historical materials, presidential records or donated historical materials located in the National Archives of the United States, a presidential library, or any other approved repository.

Subpart B—Identification and Markings

§ 2001.11 Classification authority [1.4].

(a) General.

Subpart C—Self-Inspections

§ 2001.12 Duration of classification [1.6].

Subpart D—Security Education and Training

§ 2001.13 Classification challenges [1.9].

(a) General.

Subpart E—Declassification

§ 2001.14 Classification guides [2.3].

Subpart F—Reporting

§ 2001.15 Classification defined in [2.3].

APPENDIX A TO PART 2001—INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL BYLAWS.

AUTHORITY: Section 5.2 (a) and (b), and section 5.4., E.O. 12958, 60 FR 19625, April 20, 1995.

SOURCE: 60 FR 53492, Oct. 13, 1995, unless otherwise noted.

§ 2001.11 Classification authority [1.4].

(a) General. Agencies with original classification authority shall establish
§ 2001.12 a training program for original classifiers in accordance with subpart D of this part.

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

§ 2001.12 Duration of classification

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

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

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

(iii) The original classification authority may assign an exemption designation to the information only if the information qualifies for exemption from automatic declassification as described in section 1.6(d) of the Order. Unless declassified earlier, information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.4 of the Order.

(2) Extending duration of classification for information originally classified under the Order. Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event. If an original classification authority has assigned a date or event for declassification that is 10 years or less from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for additional periods not to exceed 10 years at a time.

(i) For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information’s origin. Continued classification of this information beyond 25 years is governed by section 3.4 of the Order.

(ii) For information in records not determined to have permanent historical value, successive extensions may exceed 25 years from the date of the information’s origin.

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

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

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

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

(b) Information classified under prior orders—(1) Specific date or event. Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. However, if the information is contained in records determined by the Archivist of the United States to be permanently valuable, and the
prescribed date or event will take place more than 25 years from the information’s origin, the declassification of the information will instead be subject to section 3.4 of the Order.

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

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

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

(iii) Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.4 of the Order.

(c) Foreign government information. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. Depending on the age of the information and whether it is contained in permanently valuable records, the declassifying agency shall also determine if another exemption under section 1.6(d) (other than section 1.6(d)(5)) or 3.4(b) of the Order, such as the exemptions that pertain to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

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

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

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

§ 2001.13 Classification challenges

(a) Challenging classification. Authorized holders wishing to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific classified information in accordance with section 4.2(g) 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 for a decision. The challenger may also forward the challenge to the Interagency Security Classification Appeals 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 Interagency Security Classification Appeals 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 its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

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

§ 2001.14 Classification guides [2.3].

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

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

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

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

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

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

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

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

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

(8) Prescribe declassification instructions or the exemption category from automatic declassification for each element of information;

(9) Specify, when citing the exemption category listed in section 1.6(d)(8) of the Order, the applicable statute, treaty or international agreement;

(10) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.5 of the Order.

(c) Dissemination of classification guides. Classification guides shall be
Information Security Oversight Office, NARA

§ 2001.21

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

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

Subpart B—Identification and Markings

§ 2001.20 General [1.7].

A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after October 14, 1995, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

§ 2001.21 Original classification [1.7(a)].

(a) Primary markings. On the face of each originally classified document, including electronic media, the classifier shall apply the following markings.

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

Classified By: David Smith, Chief, Division 5

or

Classified By: ID# IMNO1, Chief, Division 5

(2) Agency and office of origin. If not otherwise evident, the agency and office of origin shall be identified and placed below 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 classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in section 1.5 of the Order.

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

(a) military plans, weapons, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security;
(f) United States Government programs for safeguarding nuclear materials or facilities; or
(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

(ii) An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: Vulnerabilities or capabilities of plans relating to the national security or Reason: 1.5(g)

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

(4) Declassification instructions. The duration of the original classification decision shall be placed on the “Declassify On” line. The classifier will apply one of the following instructions.
§ 2001.21

12 CFR Ch. XX (7–1–01 Edition)

(i) The classifier will apply a date or event for declassification that corresponds to the lapse of the information’s national security sensitivity, which may not exceed 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: October 14, 2004 or December 31, 2010

(ii) When a specific date or event within 10 years cannot be established, the classifier will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 1995, mark the “Declassify On” line as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: October 14, 2005

(iii) Upon the determination that the information must remain classified beyond 10 years, the classifier will apply the letter “X” plus the number that corresponds to that exemption category(ies) in section 1.6(d) of the Order.

(A) Exemption categories in E.O. 12958.

X1: reveal an intelligence source, method, or activity, or a cryptologic system or activity;
X2: reveal information that would assist in the development or use of weapons of mass destruction;
X3: reveal information that would impair the development or use of technology within a United States weapons system;
X4: reveal United States military plans, or national security emergency preparedness plans;
X5: reveal foreign government information;
X6: damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b) above, [section 1.6(b) of the Order];
X7: impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized;
X8: violate a statute, treaty, or international agreement.

(B) Example. A document containing information exempted from automatic declassification may appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: X-U.S. military plans or December 31, 2004

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

1. Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

2. For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked “Secret,” and other information marked “Confidential,” the overall marking would be “Secret.”

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

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

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

2. Unless the original classification authority indicates otherwise on the document, each classified portion of a document exempted from automatic
declassification shall be presumed to be exempted from automatic declassification also.

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

(d) Classification extensions. (1) An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of the information’s origin.

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

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

(4) An example of an extended duration of classification may appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: Classification extended on December 1, 2000, until December 1, 2010, by David Jones, Chief, Division 5

(e) Marking information exempted from automatic declassification at 25 years. (1) When an agency head or senior agency official exempts permanently valuable information from automatic declassification at 25 years, the “Declassify On” line shall be revised to include the symbol “25X” plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.4(b) of the Order. Other than when the exemption pertains to the identity of a confidential human source, or a human intelligence source, the revised “Declassify On” line shall also include the new date or event for declassification.

(2) The pertinent exemptions, using the language of section 3.4(b) of the Order, are:

25X1: reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;
25X2: reveal information that would assist in the development or use of weapons of mass destruction;
25X3: reveal information that would impair U.S. cryptologic systems or activities;
25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;
25X5: reveal actual U.S. military war plans that remain in effect;
25X6: reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
25X9: violate a statute, treaty, or international agreement.

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

Declassify On: 25X-State-of-the-art technology within U.S. weapon system, October 1, 2010 or
Declassify On: 25X4, October 1, 2010

(4) Documents should not be marked with a “25X” marking until the agency has been informed that the President or the Interagency Security Classification Appeals Panel concurs with the proposed exemption.

(5) Agencies need not apply a “25X” marking to individual documents contained in a file series exempted from automatic declassification under section 3.4(c) of the Order until the individual document is removed from the file.
§ 2001.22 Derivative classification [2.2].

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

(b) Source of derivative classification.
(1) The derivative classifier shall concisely identify the source document or the classification guide on the “Derived From” line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as:
Derived From: Memo, “Funding Problems,” October 20, 1995, Ofc. of Admin., Department of Good Works or
Derived From: CG No. 1, Department of Good Works, dated October 20, 1995

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

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

(2) A document derivatively classified on the basis of a source document that is itself marked “Multiple Sources” shall cite the source document on its “Derived From” line rather than the term “Multiple Sources.” An example might appear as:
Derived From: Report entitled, “New Weapons,” dated October 20, 1995, Department of Good Works, Office of Administration

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

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

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

(i) When a document is classified derivatively from a source document(s) or classification guide that contains the declassification instruction, “Originating Agency’s Determination Required,” or “OADR,” unless otherwise instructed by the original classifier, the derivative classifier shall carry forward:

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

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

(ii) An example might appear as:
Declassify On: Source marked “OADR”, Date of source: October 20, 1990

(iii) This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under section 3.4 of the Order.

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

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

§ 2001.23 Additional requirements [1.7].

(a) Marking prohibitions. Markings other than “Top Secret,” “Secret,” and “Confidential,” such as “For Official Use Only,” or “Limited Official Use,” shall not be used to identify classified national security information. No other term or phrase shall be used in conjunction with these markings, such as “Secret Sensitive” or “Agency
Confidential.” to identify classified national security information. The terms “Top Secret,” “Secret,” and “Confidential” should not be used to identify non-classified executive branch information.

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

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

Unclassified When Classified Enclosure Removed or Upon Removal of Attachments. This Document is (Classification Level)

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

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

1. Released by the originator outside the originating activity;
2. Retained more than 180 days from the date of origin; or
3. Filed permanently.

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

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

§ 2001.24 Declassification markings [Reserved].

Subpart C—Self-Inspections

§ 2001.30 General [5.6].

(a) Purpose. This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the agency’s
§ 2001.31 Coverage [5.6(c)(4)].

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

(b) Elements of coverage—(1) Original classification. (i) Evaluate original classifiers’ general understanding of the process of original classification, including the:

(A) Applicable standards for classification;

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

(C) Required classification markings.

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

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

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

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

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

(iii) Assess original classifiers’ familiarity with the duration of classification requirements, including:

(A) Assigning a specific date or event for declassification when possible;

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

(C) Limiting extensions of classification for specific information not to exceed 10 years at a time; and

(D) Exempting from declassification within 10 years specific information as provided in section 1.6 of the Order.

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

(v) Evaluate classifiers’ actions to comply with the standards specified in §§2001.14 and 2001.53 of this part, relating to classification and declassification guides, respectively.

(vi) Verify observance with the prohibitions on classification and limitations on reclassification.
(vii) Assess whether the agency’s classification challenges program meets the requirements of the Order and this part.

(2) Derivative classification. Assess the general familiarity of individuals who classify derivatively with the:
(i) Conditions for derivative classification;
(ii) Requirement to consult with the originator of the information when questions concerning classification arise;
(iii) Proper use of classification guides; and
(iv) Proper and complete application of classification markings to derivatively classified documents.

(3) Declassification. (i) Verify whether the agency has established, to the extent practical, a system of records management to facilitate public release of declassified documents.
(ii) Evaluate the status of the agency declassification program, including the requirement to:
(A) Comply with the automatic declassification provisions regarding historically valuable records over 25 years old;
(B) Declassify, when possible, historically valuable records prior to accession into the National Archives;
(C) Provide the Archivist with adequate and current declassification guides;
(D) Ascertain that the agency’s mandatory review program conforms to established requirements; and
(E) Determine whether responsible agency officials are cooperating with the Archivist in the development and maintenance of a Government-wide database of information that has been declassified.

(4) Safeguarding. (i) Monitor agency adherence to established safeguarding standards.
(ii) Assess compliance with controls for access to classified information.
(iii) Evaluate the effectiveness of the agency’s program in detecting and processing security violations and preventing recurrences.
(iv) Assess compliance with the procedures for identifying, reporting and processing unauthorized disclosures of classified information.

(v) Evaluate the effectiveness of procedures to ensure that:
(A) The originating agency exercises control over the classified information it generates;
(B) Holders of classified information do not disclose information originated by another agency without that agency’s authorization; and
(C) Departing or transferred officials return all classified information in their possession to authorized agency personnel.

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

(6) Management and oversight. (i) Determine whether original classifiers have received prescribed training.
(ii) Verify whether the agency’s special access programs:
(A) Adhere to specified criteria in the creation of these programs;
(B) Are kept to a minimum;
(C) Provide for the conduct of internal oversight; and
(D) Include an annual review of each program to determine whether it continues to meet the requirements of the Order.
(iii) Assess whether:
(A) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;
(B) Producers and users of classified information receive guidance with respect to security responsibilities and requirements;
(C) Controls to prevent unauthorized access to classified information are effective;
(D) Contingency plans are in place for safeguarding classified information used in or near hostile areas;
(E) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: Original classifiers; security managers; classification
management officers; and security specialists; and other employees significantly involved with classified information; and

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

Subpart D—Security Education and Training

§ 2001.40 General [5.6].

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

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

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

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

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

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

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

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

§ 2001.41 Coverage [5.6(c)(3)].

(a) General. Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original 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. These standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this part according to the agency’s program and policy needs.

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

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

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

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

(2) Elements of classifying and declassifying information. (i) What is classified...
Information Security Oversight Office, NARA

§ 2001.41

Information and why is it important to protect it?

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

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

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

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

(3) Elements of safeguarding. (i) What are the proper procedures for safeguarding classified information?

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

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

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

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

(1) Original classifiers. (i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

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

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

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

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

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

(2) Declassification authorities other than original classifiers. (i) What are the standards, methods and procedures for declassifying information under Executive Order 12958?

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

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

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

(3) Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information. (i) What are the original and derivative classification processes and the standards applicable to each?

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

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

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

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

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

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

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

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

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

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

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

1. Practices applicable to U.S. officials traveling overseas;
2. Procedures for protecting classified information processed and stored in automated information systems;
3. Methods for dealing with uncleared personnel who work in proximity to classified information;
4. Responsibilities of personnel serving as couriers of classified information; and
5. Security requirements that govern participation in international programs.

§ 2001.50

32 CFR Ch. XX (7–1–01 Edition)

**Subpart E—Declassification**

§ 2001.50 **Definition [3.1].**

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

§ 2001.51 **Automatic declassification [3.4].**

(a) **General.** All departments and agencies that have original classification authority, or previously had original classification authority, and maintain records appraised as having permanent historical value that contain information classified by that agency shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in carrying out an automatic declassification program involving accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States. The Archivist will not declassify information created by another agency without the prior consent of that agency.

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

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

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

(e) Processing records originated by another agency. When an agency uncovers classified records originated by another agency that appear to meet the criteria for the application of the automatic declassification provisions of the Order, the finding agency should alert the originating agency and seek instruction regarding the handling and disposition of pertinent records.

(f) Unscheduled records. Classified information in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.4 of the Order. Classified information in records that are scheduled as permanently valuable when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order five years from the date the records are scheduled. Classified information in records that are scheduled as permanently valuable when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order when the information is 25 years old.

(g) Foreign government information. The declassifying agency is the agency that initially received or classified the information. When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency shall also determine if another exemption under section 3.4(b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

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

(i) Use of approved declassification guides. Approved declassification guides may be used as a tool to assist in the exemption from automatic declassification of specific information as provided in section 3.4(d) of the Order. These guides must include additional pertinent detail relating to the exemptions described in section 3.4(b) of the Order, and follow the format required of declassification guides for systematic review as described in §2001.53 of this part. In order for such guides to be used in place of the identification of specific information within individual documents, the information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions for general categories of information will not be acceptable. The actual items to be exempted are specific documents. All such declassification guides used in conjunction with section 3.4(d) of the Order must be submitted to the Director of ISOO.
§ 2001.52 Systematic declassification review [3.5].

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

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

§ 2001.53 Declassification guides [3.5(b)].

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

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

(1) Identify the subject matter of the declassification guide;
(2) Identify the original declassification authority by name or personal identifier, and position;
(3) Provide the date of issuance or last review;
(4) State precisely the categories or elements of information:
   (i) To be declassified;
   (ii) To be downgraded; or
   (iii) Not to be declassified.
(5) Identify any related files series that have been exempted from automatic declassification pursuant to section 3.4(c) of the Order;
(6) To the extent a guide is used in conjunction with the automatic declassification provisions in section 3.4 of the Order, state precisely the elements of information to be exempted from declassification to include:
   (i) The appropriate exemption category listed in section 3.4(b) of the Order, and, when citing the exemption category listed in section 3.4(b)(9) of the Order, specify the applicable statute, treaty or international agreement; and
   (ii) A date or event for declassification.
(c) External review. Agencies shall submit declassification guides for review to the Director of ISOO. To the extent such guides are used in conjunction with the automatic declassification provisions in section 3.4 of the Order, the Director shall submit them...
§ 2001.54 Mandatory review for declassification [3.6, 3.7].

(a) U.S. originated information—(1) Receipt of requests. Each agency shall publish in the FEDERAL REGISTER the identity of the person(s) or office(s) to which mandatory declassification review requests should be addressed.

(2) Processing. (i) Requests for classified records in the custody of the originating agency. A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. In responding to mandatory declassification review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. Agencies shall ordinarily make a final determination within 180 days from the date of receipt. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) Requests for classified records in the custody of an agency other than the originating agency. When an agency receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall process the request in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency.

(iii) Appeals of denials of mandatory declassification review requests. The agency appellate authority shall normally make a determination within 60 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(iv) Appeals to the Interagency Security Classification Appeals Panel. In accordance with section 5.4 of the Order, the Interagency Security Classification Appeals Panel shall publish in the FEDERAL REGISTER no later than February 12, 1996, the rules and procedures for bringing mandatory declassification appeals before it.

(b) Foreign government information. Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with this section. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency shall also determine if another exemption under section 1.6(d) of the Order (other than section 1.6(b)(5)), such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such
an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

(c) Cryptologic and intelligence information. Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(d) Fees. In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 9701 of title 31, United States Code. The schedules of fees published in the \textit{Federal Register} by agencies in implementation of Executive Order 12336 shall remain in effect until revised.

(e) Assistance to the Department of State. Heads of agencies should assist the Department of State in its preparation of the \textit{Foreign Relations of the United States} (FRUS) series by facilitating access to appropriate classified materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

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

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

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


(a) Purpose. Under E.O. 12958, agencies reviewing records for declassification must facilitate the review of equities of other agencies contained in their records. Because agencies have a variety of processes for review and referral, common language and standards are needed to ensure clear, concise communication and coordinated action among all agencies involved in the referral process. Common language and standards are needed for declassification, exemption from automatic declassification, and proper marking of information subject to the automatic declassification provision of the Order. Consistent declassification of information through standardized procedures should result in lower cost and greater process efficiency, review accuracy, and the protection of the equities of all executive branch agencies.

(b) Applicability. These standards are binding on all executive branch agencies that create or handle classified information and are applicable to records covered under Section 3.4 of the Order. With respect to records reviewed prior to the issuance of these standards, deviations are acceptable as long as prior practice does not completely obstruct record referral.

(c) Responsibility. The senior agency official is responsible for the agency’s referral program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) Definitions. For the purpose of this section:

\textit{Declassified or Declassification} means the authorized change in the status of information from classified information to unclassified information.

\textit{Equity} means information originally classified by or under the control of an agency, as control is defined in section 1.1(b) of E.O. 12958.

\textit{Exempted} means nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under E.O. 12958.


Pass/fail (P/F) means a declassification technique that regards information at the full document level. Any exemptible portion of a document may result in exemption (failure) of the entire document. Documents that contain no exemptible information are passed and therefore declassified. Declassified documents may be subject to other FOIA exemptions other than the security exemption (§(b)(1)), and the requirements placed by legal authorities governing Presidential holdings.

Record means the statutory definition as provided under title 44 U.S.C. 3301 and 44 U.S.C. 2111, 2111 note, and 2201.

Redaction means a sanitization technique that involves removal (editing out) of exempted information from a document.

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

(e) Approaches to declassification. The exchange of information between agencies and the final disposition of documents are affected by differences in the approaches to declassification. Agencies conducting pass/fail reviews may refer documents to agencies that redact. Actions taken by the sender and the recipient may differ as noted below:

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

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

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

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

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

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

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

(g) Unmarked or improperly marked documents. Agencies that find other agency information in unmarked or improperly marked documents that have been maintained and protected as classified information must afford those documents appropriate protection and tab or refer the documents as described in paragraph (h) of this section. Agencies must provide other pertinent information, if available, regarding additional copies or possible public disclosure.

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

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

(2) Tab and notify.

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

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

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

(i) [Reserved].

(j) Reviewed document marking. Consistency in marking is essential in the referral of significant numbers of documents under the Executive Order. Decisions made during review must be communicated clearly to all subsequent reviewers.

(1) Redactions must never be indicated on original documents, only on copies. Redaction agencies need a means of tracking the results of review (at the document level) by all reviewing agencies and a reason for each redaction.

(2) If only one exemption from declassification applies to all redacted portions of a document, the applicable exemption may be indicated on the front page of the redacted copy. If more than one exemption applies to a document, each redacted portion for which an exemption is asserted must be marked on the redacted copy.

(3) Redacted portions must be marked to indicate the agency and the number of the applicable exemption, for example, DIA25X1.

(4) Agencies reviewing a referred document must indicate on the tab, folder, or box the result of the review (i.e., exemption or declassification). The original document should be marked with the final action only by the agency responsible for the final declassification decision. Options include marking a copy of the document, marking the tab, notification as part of a transmittal, or marking the box or folder according to NARA guidelines. Automated agencies may forgo marking documents, provided the required information is maintained in an agency database and is accessible to other agencies. Exempt documents may be marked.

(i) Sample Exempted Document Stamp. Exempt documents may be stamped as shown in the following example:
§ 2001.55

(A) Normally, only one stamp should be placed on the document with any subsequent reviewing agencies adding their information to the stamp on the document, if possible. The stamp should not cover any writing on the document.

(B) Specific fields in the stamp must be completed as follows:

(1) **Exemption Code:** Agency(ies) ID and 25X plus exemption code(s).

(2) **Date/Event:** A specific date or event for declassification.

(3) **Other Agency Equity:** This line is used to track other agency equtities and their review. The declassification authority enters “NONE” if no other agency equities are present, the identifiers of agencies with equity, or “TBD” (To be determined) if equities are unknown. Agency identifiers are crossed off as the reviews are completed and names may be added if additional equities are found.

(4) **Reviewed by:** Optional. If used, enter name or other personal identifier.

(5) **Date:** Enter date the action was taken.

(ii) Sample Stamp for Document Declassification. (A) When agencies mark declassified documents, the stamp must, at a minimum, include the information shown in the following example:

```
EXEMPTED PER E.O. 12958
Exemption Code: ______________
Date/Event ______________
Other Agency Equity: ______________
Reviewed By: ______________ Date: ______________
```

(B) Specific fields in the stamp must be completed as follows:

(1) **Agency:** Name of the agency.

(2) **By:** Name or personal identifier of the reviewer. (Optional)

```
DECLASSIFIED
PER E.O. 12958
Agency: ______________
By: ______________ Date: ______________
```

(3) **Date:** Date the action was taken.

[64 FR 49389, Sept. 13, 1999; 64 FR 62113, Nov. 16, 1999; 65 FR 16320, Mar. 28, 2000]
§ 2001.60 Statistical reporting [5.3].
Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director shall solicit recommendations from the member agencies of the Security Policy Forum regarding the reporting requirements. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§ 2001.61 Accounting for costs [5.6(c)(8)].
(a) Information on the costs associated with the implementation of the Order will be collected from the agencies by the Office of Management and Budget (OMB). OMB will provide data to ISOO on the cost estimates for classification-related activities. ISOO will include these cost estimates in its annual report to the President. The agency senior official should work closely with the agency comptroller to ensure that the best estimates are collected.

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

§ 2001.62 Effective date [6.2].
Part 2001 shall become effective October 14, 1995.

APPENDIX A TO PART 2001—INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL BYLAWS

ARTICLE I. PURPOSE
The purpose of the Interagency Security Classification Appeals Panel (ISCAP) and these bylaws is to fulfill the functions assigned to the ISCAP by Executive Order 12958, “Classified National Security Information.”
Information Security Oversight Office, NARA

Pt. 2001, App. A

any member or the Executive Secretary. Acting through the Executive Secretary, the Chair will distribute the agenda and supporting materials to the members as soon as possible before a scheduled meeting.

F. Minutes. The Executive Secretary shall be responsible for the preparation of each meeting’s minutes, and the distribution of draft minutes to each member. The minutes will include a record of the members present at the meeting and the result of each vote. At the subsequent meeting of the ISCAP, the Chair will read or reference the draft minutes of the previous meeting. At that time the minutes will be corrected, as necessary, and approved by the membership and certified by the Chair. The approved minutes will be maintained among the records of the ISCAP.

ARTICLE V. VOTING

A. Motions. When a decision or recommendation of the ISCAP is required to resolve a matter before it, the Chair shall request or accept a motion for a vote. Any member, including the Chair, may make a motion for a vote. No second shall be required to bring any motion to a vote. A quorum must be present when a vote is taken.

B. Eligibility. Only the members, including the Chair, may vote on a motion before the ISCAP, with each agency or office represented having one vote.

C. Voting Procedures. Votes shall ordinarily be taken and tabulated by a show of hands.

D. Passing a Motion. In response to a motion, members may vote affirmatively, negatively, or abstain from voting. Except as otherwise provided in these bylaws, a motion passes when it receives a majority of affirmative votes of the members voting. However, in no instance will the ISCAP reverse an agency’s decision without the affirmative vote of at least a majority of the members present.

E. Votes in a Non-meeting Context. In extraordinary circumstances, the Chair may call for a vote of the membership outside the context of a formal ISCAP meeting. An alternate member may also participate in such a vote if the primary member cannot. The Executive Secretary shall record and retain such votes in a documentary form and immediately report the results to the Chair and other primary and alternate members.

ARTICLE VI. FIRST FUNCTION: APPEALS OF AGENCY DECISIONS REGARDING CLASSIFICATION CHALLENGES

In accordance with section 5.4(b) of the Order, the ISCAP shall decide on appeals by authorized persons who have filed classification challenges under section 1.9 of the Order.

A. Jurisdiction. The ISCAP will consider appeals from classification challenges that otherwise meet the standards of the Order if:

1. The appeal is filed in accordance with these bylaws.

2. The appellant has previously challenged the classification action at the agency that originated or is otherwise responsible for the information in question in accordance with the agency’s procedures or, if the agency has failed to establish procedures for classification challenges, by filing a written challenge directly with the agency head or designated senior agency official, as defined in section 1.1(j) of the Order.

3. The appellant has (a) received a final agency decision denying his or her challenge; or (b) not received (i) an initial written response to the classification challenge from the agency within 120 days of filing, or (ii) a written response to an internal agency appeal within 90 days of the filing of the appeal.

4. There is no action pending in the federal courts regarding the information in question; and

5. The information in question has not been the subject of review by the federal courts or the ISCAP within the past two years.

B. Addressing of Appeals. Appeals should be addressed to: Executive Secretary, Interagency Security Classification Appeals Panel, Attn: Classification Challenge Appeals, c/o Information Security Oversight Office, National Archives and Records Administration, 7th and Pennsylvania Avenue, NW., Room 5W, Washington, DC 20408.

The appeal must contain enough information for the Executive Secretary to be able to obtain all pertinent documents about the classification challenge from the affected agency. No classified information should be included within the initial appeal document. The Executive Secretary will arrange for the transmittal of classified information from the agency after receiving the appeal. If it is impossible for the appellant to file an appeal without including classified information, prior arrangements must be made by contacting the Information Security Oversight Office.

C. Timeliness of Appeals. An appeal to the ISCAP must be filed within 60 days of:

1. The date of the final agency decision; or

2. The agency’s failure to meet the time frames established in paragraph (A)(3)(b) of this Article.

D. Rejection of Appeal. If the Executive Secretary determines that the appeal does not meet the requirements of the Order or these bylaws, the Executive Secretary shall notify the appellant in writing that the appeal will not be considered by the ISCAP. The notification shall include an explanation of why the appeal is deficient.
E. Preparation. The Executive Secretary shall notify the Chair and the designated senior agency official(s) of the affected agency(ies) when an appeal is lodged. Under the direction of the ISCAP, the Executive Secretary shall supervise the preparation of an appeal file, pertinent portions of which will be presented to the members of the ISCAP for their review prior to a vote on the appeal. The appeal file will eventually include all records pertaining to the appeal.

F. Resolution of Appeals. The ISCAP may vote to affirm the agency’s decision, to reverse the agency’s decision in whole or in part, or to remand the matter to the agency for further consideration. A decision to reverse an agency’s decision requires the affirmative vote of at least a majority of the members present.

G. Notification. The Executive Secretary shall promptly notify in writing the appellant, the agency head, and designated senior agency official of the ISCAP’s decision.

H. Agency Appeals. Within 60 days of receipt of an ISCAP decision that reverses a final agency decision, the agency head may petition the President through the Assistant to the President for National Security Affairs to overrule the decision of the ISCAP.

I. Protection of Classified Information. All persons involved in the appeal shall make every effort to minimize the inclusion of classified information in the appeal file. Any classified information contained in the appeal file shall be handled and protected in accordance with the Order and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it. In no instance will the ISCAP declassify properly classified information solely because of an agency’s failure to prescribe or follow appropriate procedures for handling classification challenges.

J. Maintenance of File. The Executive Secretary shall maintain the appeal file among the records of the ISCAP.

ARTICLE VII. SECOND FUNCTION: REVIEW OF AGENCY EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION

In accordance with section 5.4(b) of the Order, the ISCAP shall approve, deny or amend agency exemptions from automatic declassification as provided in section 3.4(d) of the Order.

A. Agency Notification of Exemptions. The agency head or designated senior agency official shall notify the Executive Secretary of agency exemptions in accordance with the requirements of the Order and its implementing directives. Agencies shall provide any additional information or justification that the Executive Secretary believes is necessary or helpful in order for the ISCAP to review and decide on the exemption. The agency head may seek relief from the ISCAP from any request for information by the Executive Secretary to which the agency objects.

B. Preparation. The Executive Secretary shall notify the Chair of the agency submission. At the direction of the ISCAP, the Executive Secretary shall supervise the preparation of an exemption file, pertinent portions of which will be presented to the members of the ISCAP for their review prior to a vote on the exemptions. The exemption file will eventually include all records pertaining to the ISCAP’s consideration of the agency’s exemptions.

C. Resolution. The ISCAP may vote to approve an agency exemption, to deny an agency exemption, to amend an agency exemption, or to remand the matter to the agency for further consideration. A decision to deny or amend an agency exemption requires the affirmative vote of a majority of the members present.

D. Notification. The Executive Secretary shall promptly notify in writing the agency head and designated senior agency official of the ISCAP’s decision.

E. Agency Appeals. Within 60 days of receipt of an ISCAP decision that denies or amends an agency exemption, the agency head may petition the President through the Assistant to the President for National Security Affairs to overrule the decision of the ISCAP.

F. Protection of Classified Information. Any classified information contained in the exemption file shall be handled and protected in accordance with the Order and its implementing directives. Information that the agency maintains is exempt from declassification shall remain classified unless and until a final decision is made to declassify it.

G. Maintenance of File. The Executive Secretary shall maintain the exemption file among the records of the ISCAP.

ARTICLE VIII. THIRD FUNCTION: APPEALS OF AGENCY DECISIONS DENYING DECLASSIFICATION UNDER MANDATORY REVIEW PROVISIONS OF THE ORDER

In accordance with section 5.4(b) of the Order, the ISCAP shall decide on appeals by parties whose requests for declassification under section 3.6 of the Order have been denied.

A. Jurisdiction. The ISCAP will consider appeals from denials of mandatory review for declassification requests that otherwise meet the standards of the Order if:

1. The appeal is filed in accordance with these bylaws;
2. The appellant has previously filed a request for mandatory declassification review at the agency that originated or is otherwise responsible for the information in question in accordance with the agency’s procedures or, if the agency has failed to establish procedures for mandatory review, by filing a...
written request directly with the agency head or designated senior agency official;

3. The appellant has
   (a) Received a final agency decision denying its request for declassification; or
   (b) Not received (i) an initial decision on the request for mandatory declassification review from the agency within one year of its filing, or (ii) a final decision on an internal agency appeal within 180 days of the filing of the appeal;

4. There is no action pending in the federal courts regarding the information in question; and

5. The information in question has not been the subject of review by the federal courts or the ISCAP within the past two years.

B. Addressing of Appeals. Appeals should be addressed to: Executive Secretary, Interagency Security Classification Appeals Panel, Attn: Mandatory Review Appeals, c/o Information Security Oversight Office, National Archives and Records Administration, 7th and Pennsylvania Avenue, NW., Room SW 501, Washington, DC 20408.

The appeal must contain enough information for the Executive Secretary to be able to obtain all pertinent documents about the request for mandatory declassification review from the affected agency.

C. Timeliness of Appeals. An appeal to the ISCAP must be filed within 60 days of:
   1. The date of the final agency decision; or
   2. The agency’s failure to meet the time frames established in paragraph (A)(3)(b) of this Article.

D. Rejection of Appeal. If the Executive Secretary determines that the appeal does not meet the requirements of the Order or these bylaws, the Executive Secretary shall notify the appellant in writing that the appeal will not be considered by the ISCAP. The notification shall include an explanation of why the appeal is deficient.

E. Preparation. The Executive Secretary shall notify the Chair and the designated senior agency official(s) of the affected agency(ies) when an appeal is lodged. Under the direction of the ISCAP, the Executive Secretary shall supervise the preparation of an appeal file, pertinent portions of which will be presented to the members of the ISCAP for their review prior to a vote on the appeal. The appeal file will eventually include all records pertaining to the appeal.

F. Narrowing Appeals. To expedite the resolution of appeals and minimize backlogs, the Executive Secretary is authorized to consult with appellants with the objective of narrowing or prioritizing the information subject to the appeal.

G. Resolution of Appeals. The ISCAP may vote to affirm the agency’s decision, to reverse the agency’s decision in whole or in part, or to remand the matter to the agency for further consideration. A decision to reverse an agency’s decision requires the affirmative vote of at least a majority of the members present.

H. Notification. The Executive Secretary shall promptly notify in writing the appellant, the agency head, and designated senior agency official of the ISCAP’s decision.

I. Agency Appeals. Within 60 days of receipt of an ISCAP decision that reverses a final agency decision, the agency head may petition the President through the Assistant to the President for National Security Affairs to overrule the decision of the ISCAP.

J. Protection of Classified Information. All persons involved in the appeal shall make every effort to minimize the inclusion of classified information in the appeal file. Any classified information contained in the appeal file shall be handled and protected in accordance with the Order and its implementing directives. Information that is subject to an appeal from an agency decision denying declassification under the mandatory review provisions of the Order shall remain classified unless and until a final decision is made to declassify it. In no instance will the ISCAP declassify properly classified information solely because of an agency’s failure to prescribe or follow appropriate procedures for handling mandatory review for declassification requests and appeals.

K. Maintenance of File. The Executive Secretary shall maintain the appeal file among the records of the ISCAP. All information declassified as a result of ISCAP action shall be available for inclusion within the database established by the Archivist of the United States in accordance with section 3.8 of the Order.

ARTICLE IX. ADDITIONAL FUNCTIONS

In its consideration of the matters before it, the ISCAP shall perform such additional advisory functions as are consistent with and supportive of the successful implementation of the Order.

ARTICLE X. SUPPORT STAFF

As provided in section 5.4(a) of the Order, the Director of the Information Security Oversight Office will serve as Executive Secretary to the ISCAP, and the staff of the Information Security Oversight Office will provide program and administrative support for the ISCAP. The Executive Secretary will supervise the staff in this function pursuant to the direction of the Chair and ISCAP. On an as needed basis, the ISCAP may seek details from its member agencies to augment the staff of the Information Security Oversight Office in support of the ISCAP.

ARTICLE XI. RECORDS

A. Integrity of ISCAP Records. The Executive Secretary shall maintain separately documentary materials, regardless of their
§ 2002.1 Purpose.

These general guidelines for the systematic declassification review of foreign government information have been developed in accordance with the provisions of section 3.3 of Executive Order 12356, “National Security Information,” and §2001.31 of Information Security Oversight Office Directive No. 1. All foreign government information that has been incorporated into the permanently valuable records of the United States Government and that has been accessioned into the National Archives of the United States shall be systematically reviewed for declassification by the Archivist of the United States. Declassification reviews shall be conducted in accordance with the provisions of these general guidelines or, if available, in accordance with specific systematic review guidelines for foreign government information provided by the agency heads who have declassification authority over that information. All foreign government information—

(a) Not identified in §2002.6 of these general guidelines or in specific agency guidelines as requiring item-by-item declassification review and final determination by an agency declassification authority, and

(b) For which a prior declassification date has not been established, shall be declassified as that information becomes thirty years old.

§ 2002.2 Definition.

Foreign government information as used in these guidelines means:

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

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

§ 2002.3 Scope.

(a) These guidelines apply to foreign government information that has been received or classified by the United
States Government or its agents, and has been incorporated into records determined by the Archivist of the United States to have permanent value.

(b) Atomic energy information (including information originated prior to 1947 and not marked as such; information received from the United Kingdom or Canada marked “Atomic,” or information received from NATO marked “Atomal”) that is defined and identified as “Restricted Data” or “Formerly Restricted Data” in Sections 11y and 142d of the Atomic Energy Act of 1954, as amended, is outside the scope of these guidelines. Such information is not subject to systematic review and may not be automatically downgraded or declassified. Any document containing information within the definition of “Restricted Data” or “Formerly Restricted Data” that is not so marked shall be referred to the Department of Energy Office of Classification for review and appropriate marking, except for licensing and related regulatory matters which shall be referred to the Division of Security, U.S. Nuclear Regulatory Commission.

§ 2002.4 Responsibilities.

(a) Foreign government information transferred to the General Services Administration for accession into the National Archives of the United States shall be reviewed by the Archivist of the United States for declassification in accordance with Executive Order 12356, the directives of the Information Security Oversight Office, these general guidelines, and any specific systematic declassification guidelines provided by the agency with declassification authority over the information.

(b) Accessioned foreign government information in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and cryptology records created after 1945, shall be subject to review by the Archivist for declassification as it becomes 50 years old. All other accessioned foreign government information shall be subject to review by the Archivist for declassification as it becomes 30 years old.

(c) Agency heads who have declassification jurisdiction over permanently valuable foreign government information in agency records not yet accessioned into the National Archives of the United States are encouraged to conduct systematic declassification reviews of it in accordance with the time limits specified in paragraph (b) of this section. These reviews shall comply with the provisions of Executive Order 12356, the directives of the Information Security Oversight Office, these general guidelines, and specific agency systematic review guidelines that have been issued in consultation with the Archivist of the United States and the ISOO Director.

(d) Foreign government information falling within any of the categories listed in §2002.6 of these guidelines shall be declassified or downgraded only upon specific authorization of the agency that has declassification authority over it. Such information shall be referred to the responsible agency(ies) for review. Information so referred shall remain classified until the responsible agency(ies) has declassified it. If the responsible agency cannot be readily identified from the document or material, referral shall be made in accordance with §2002.7 of these guidelines.

(e) When required, the agency having declassification authority over the information shall consult with foreign governments concerning its proposed declassification.

§ 2002.5 Effect of publication.

(a) Foreign government information shall be considered declassified when published in an unclassified United States Government executive branch publication (e.g., the Foreign Relations of the United States series) or when cleared for publication by United States Government executive branch officials authorized to declassify the information; or if officially published as unclassified by the foreign government(s) or international organization(s) of governments that furnished the information unless the fact of the U.S. Government’s possession of the information requires continued protection.
§ 2002.6 Categories requiring item-by-item review.

Foreign government information falling into the following categories require item-by-item review for declassification by agencies having declassification authority over it.

(a) Information exempted from declassification under any joint arrangement evidenced by an exchange of letters, memorandum of understanding, or other written record, with the foreign government or international organization of governments, or element(s) thereof, that furnished the information. Questions concerning the existence or applicability of such arrangements shall be referred to the agency or agencies having declassification authority over the records under review.

(b) Information related to the safeguarding of nuclear materials or facilities, foreign and domestic, including but not necessarily limited to vulnerabilities and vulnerability assessments of nuclear facilities and Special Nuclear Material.

(c) Nuclear arms control information (see also paragraph (k) of this section).

(d) Information regarding foreign nuclear programs (other than "Restricted Data" and "Formerly Restricted Data"), such as:

   (1) Nuclear weapons testing.
   (2) Nuclear weapons storage and stockpile.
   (3) Nuclear weapons effects, hardness, and vulnerability.
   (4) Nuclear weapons safety.
   (5) Cooperation in nuclear programs including, but not limited to, peaceful and military applications of nuclear energy.
   (6) Exploration, production and import of uranium and thorium from foreign countries.

(e) Information concerning intelligence activities (including special activities) or intelligence or counterintelligence sources or methods including but not limited to intelligence, counterintelligence and covert action programs, plans, policies, operations, or assessments; or which would reveal or identify:

   (1) Any present, past or prospective undercover personnel, installation, unit, or clandestine human agent, of the United States or a foreign government;
   (2) Any present, past or prospective method, procedure, mode, technique or requirement used or being developed by the United States or by foreign governments, individually or in combination to produce, acquire, transmit, analyze, correlate, assess, evaluate or process intelligence or counterintelligence, or to support an intelligence or counterintelligence source, operation, or activity;
   (3) The present, past or proposed existence of any joint United States and foreign government intelligence, counterintelligence, or covert action activity or facility, or the nature thereof.

(For guidance on protecting United States foreign intelligence liaison relationships, see Director of Central Intelligence Directive “Security Classification Guidance and Foreign Security Services,” effective January 18, 1982.)

(f) Information that could result in or lead to actions which would place an individual in jeopardy attributable to disclosure of the information, including but not limited to:

   (1) Information identifying any individual or organization as a confidential source of intelligence or counterintelligence.
(2) Information revealing the identity of an intelligence or covert action agent or agents.

(3) Information identifying any individual or organization used to develop or support intelligence, counterintelligence, or covert action agents, sources or activities.

(g) Information about foreign individuals, organizations or events which if disclosed, could be expected to:

(1) Adversely affect a foreign country’s or international organization’s present or future relations with the United States.

(2) Adversely affect present or future confidential exchanges between the United States and any foreign government or international organization of governments.

(h) Information related to plans (whether executed or not, whether presented in whole or in part), programs, operations, negotiations, and assessments shared by one or several foreign governments with the United States, including but not limited to those involving the territory, political regime or government of another country, and which if disclosed could be expected to adversely affect the conduct of U.S. foreign policy or the conduct of another country’s foreign policy with respect to a third country or countries. This item would include contingency plans, plans for covert political, military or paramilitary activities or operations by a foreign government acting alone or jointly with the United States Government, and positions or actions taken by a foreign government alone or jointly with the United States concerning border disputes or other territorial issues.

(i) Information concerning arrangements with respect to foreign basing of cryptologic operations and/or foreign policy considerations relating thereto.

(j) Scientific information such as that concerning space, energy, climatology, communications, maritime, undersea, and polar projects, the disclosure of which could be expected to adversely affect current and/or future exchanges of such information between the United States and any foreign governments or international organizations of governments.

(k) Information on foreign policy aspects of nuclear matters, the disclosure of which could be expected to adversely affect cooperation between one or more foreign governments and the United States Government.

(l) Information concerning physical security arrangements, plans or equipment for safeguarding United States Government embassies, missions or facilities abroad, the disclosure of which could reasonably be expected to increase the vulnerability of such facilities to penetration, attack, take-over, and the like.

(m) Nuclear propulsion information.

(n) Information concerning the establishment, operation, and support of nuclear detection systems.

(o) Information concerning or revealing military or paramilitary escape, evasion, cover or deception plans, procedures, and techniques, whether executed or not.

(p) Information which could adversely affect the current or future usefulness of military defense policies, programs, weapons systems, operations, or plans.

(q) Information concerning research, development, testing and evaluation of chemical and biological weapons and defense systems; specific identification of chemical and biological agents and munitions; and chemical and biological warfare plans.

(r) Technical information concerning weapons systems and military equipment that reveals the capabilities, limitations, or vulnerabilities of such systems, or equipment that could be exploited to destroy, counter, render ineffective or neutralize such weapons or equipment.

(s) Cryptologic information, including cryptologic sources and methods, currently in use. This includes information concerning or revealing the processes, techniques, operations, and scope of signals intelligence comprising communications intelligence, electronic intelligence, and telemetry intelligence, the cryptosecurity and emission security components of communications security, and the communications portion of cover and deception plans.

(t) Information concerning electronic warfare (electronic warfare support
§ 2002.7  Referral and decision.

(a) When the identity of the agencies having declassification authority over foreign government information is not apparent to the agency holding the information, or when reviewing officials do not possess the requisite expertise, the information shall be referred for review and a declassification determination as follows:

1. Categories 2002.6 (b) through (d), Department of Energy or Nuclear Regulatory Commission (as appropriate).
2. Categories 2002.6 (e) and (f), Central Intelligence Agency.
3. Categories 2002.6 (g) through (l), Department of State.
4. Categories 2002.6 (m) through (t), Department of Defense.
5. Categories 2002.6 (u) and (w), Department of the Treasury.

(b) Referrals to agencies shall include copies of the documents containing the
§ 2003.4 Availability.

Agencies may obtain copies of the standard forms prescribed in subpart B by ordering through FEDSTRIP/MILSTRIP or from the General Services Administration (GSA) Customer Supply Centers (CSCs). The national stock number of each form is cited with its description in subpart B.

[50 FR 51826, Dec. 19, 1985]
Subpart B—Prescribed Forms


(a) SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information. From the effective date of this rule, September 29, 1988, the SF 312 shall be used in lieu of both the SF 189 and the SF 189-A for this purpose. In any instance in which the language in the SF 312 differs from the language in either the SF 189 or SF 189-A, agency heads shall interpret and enforce the SF 189 or SF 189-A in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

(b) All employees of executive branch departments, and independent agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(c) All Government contractor, licensee, grantee, or other non-Government personnel requiring access to classified information in the performance of their duties, who have not previously signed either the SF 189 or the SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(d) Agencies may require other persons, who are not included under paragraphs (b) or (c) of this section, and who have not previously signed either the SF 189 or the SF 189-A, to execute SF 312 before receiving access to classified information. A person in such circumstances who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(e) The use of the “Security Debriefing Acknowledgement” portion of the SF 312 is optional at the discretion of the implementing agency.

(f) 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.

(g) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of section 2302, title 5, United States Code, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(h)(1) Modification of the SF 189. The second sentence of paragraph 1 of every executed copy of the SF 189 is clarified to read:

As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards
for classification and is in the process of a classification determination as provided in sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security.

(2) Scope of "classified information". As used in the SF 312, the SF 189, and the SF 189–A, "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in sections 1.1(c) and 1.2(e) of Executive Order 12356 or any other statute or Executive order that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification and is currently in the process of a classification determination.

(3) Basis for liability. A party to the SF 312, SF 189 or SF 189–A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (i) The marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (ii) his or her action will result, or reasonably could result in the unauthorized disclosure of that information.

In no instance may a party to the SF 312, SF 189 or SF 189–A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

(4) Modification of the SF 312, SF 189 and SF 189–A.

(i) Each executed copy of the SF 312, SF 189 and SF 189–A, whether executed prior to or after the publication of this rule, is amended to include the following paragraphs 10 and 11.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; section 7211 of title 5 U.S.C. (governing disclosures to Congress); section 1034 of title 10 U.S.C., as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5 U.S.C., as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18 U.S.C. and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR 2003.20) so that I may read them at this time, if I so choose.

(ii) The first sentence of paragraph 7 of each executed copy of the SF 312, SF 189 and SF 189–A, whether executed prior to or after the publication of this rule, is amended to read:

I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of, the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law.

The second sentence of paragraph 7 of each executed copy of the SF 312 (September 1988 version), SF 189 and SF 189–A, which reads, “I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information,” and whether executed prior to or after the publication of this rule, is deleted.

(1) Points of clarification. (i) As used in paragraph 3 of SF 189 and SF 189–A, the word “indirect” refers to any situation in which the knowing, willful or negligent action of a party to the agreement results in the unauthorized disclosure of classified information even though the party to the agreement does not directly communicate, deliver or transmit classified information to a

(a) 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.

(b) SF 700 shall be used in all situations that call for the use of a security container information form. Agency-wide use of SF 700 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.

(c) 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 as required by applicable executive order(s), statute(s) or implementing security regulations.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant an agency’s request for a waiver from the use of SF 700. To apply for a waiver, an agency must submit its proposed alternative non-disclosure agreement to the Director of ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement’s enforceability from the Department of Justice and may provide a recommendation to the National Security Council. An agency that has previously received a waiver from the use of the SF 189 or the SF 189–A need not seek a waiver from the use of the SF 312.

(e) Only the National Security Council 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 non-disclosure agreement to the Director of ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement’s enforceability from the Department of Justice and may provide a recommendation to the National Security Council. An agency that has previously received a waiver from the use of the SF 189 or the SF 189–A need not seek a waiver from the use of the SF 312.

(a) 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.

(b) SF 701 shall be used in all situations that call for the use of an activity security checklist. Agency-wide use of SF 701 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.

(c) Completion, storage and disposition of SF 701 will be in accordance with each agency’s security regulations.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant an agency’s application for a waiver from the use of SF 701. 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 ISOO Director will review the request and notify the agency of the decision.

(e) The national stock number for the SF 701 is 7540–01–213–7899.

[50 FR 51826, Dec. 19, 1985]


(a) SF 702 provides a record of the names and times that persons have opened, closed or checked a particular container that holds classified information.

(b) SF 702 shall be used in all situations that call for the use of a security container check sheet. Agency-wide use of SF 702 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.

(c) Completion, storage and disposition of SF 702 will be in accordance with each agency’s security regulations.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant an agency’s application for a waiver from the use of SF 702. 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 ISOO Director will review the request and notify the agency of the decision.

(e) The national stock number for the SF 702 is 7540–01–213–7900.

[50 FR 51826, Dec. 19, 1985]

§ 2003.24 TOP SECRET Cover Sheet: SF 703.

(a) 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.

(b) SF 703 shall be used in all situations that call for the use of a TOP SECRET cover sheet. Agency-wide use of SF 703 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.

(c) SF 703 is affixed to the top of the TOP SECRET document and remains attached until the document is destroyed. At the time of destruction, SF 703 is removed and, depending upon its condition, reused.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant any agency’s application for a waiver from the use of SF 703. 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 ISOO Director will review the request and notify the agency of the decision.

(e) The national stock number for the SF 703 is 7540–01–213–7901.

[50 FR 51826, Dec. 19, 1985]

§ 2003.25 SECRET Cover Sheet: SF 704.

(a) 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.

(b) SF 704 shall be used in all situations that call for the use of a SECRET cover sheet. Agency-wide use of SF 704 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.
§ 2003.26

(c) SF 704 is affixed to the top of the SECRET document and remains attached until the document is destroyed. At the time of destruction, SF 704 is removed and, depending upon its condition, reused.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant any agency’s application for a waiver from the use of SF 704. 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 ISOO Director will review the request and notify the agency of the decision.

(e) The national stock number of the SF 704 is 7540–01–213–7902.

[50 FR 51827, Dec. 19, 1985]

§ 2003.26 CONFIDENTIAL Cover Sheet: SF 705.

(a) 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.

(b) SF 705 shall be use in all situations that call for the use of a CONFIDENTIAL cover sheet. Agency-wide use of SF 705 shall begin when supplies of existing forms are exhausted or September 30, 1986, whichever occurs earlier.

(c) SF 705 is affixed to the top of the CONFIDENTIAL document and remains attached until the document is destroyed. At the time of destruction, SF 705 is removed and, depending upon its condition, reused.

(d) Only the Director of the Information Security Oversight Office (ISOO) may grant any agency’s application for a waiver from the use of SF 705. 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 ISOO Director will review the request and notify the agency of the decision.

(e) The national stock number of the SF 705 is 7540–01–207–5536.

[52 FR 10190, Mar. 30, 1987]

§ 2003.28 SECRET Label SF 707.

(a) SF 707 is used to identify and protect automatic data processing (ADP) media and other media that contain SECRET information. SF 707 is used instead of the SF 704 for media other than documents.

(b) SF 707 shall be used in all situations that call for the use of a TOP SECRET Label. Agency-wide use of SF 707 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) SF 707 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.

(d) Only the Director of ISOO may grant a waiver from the use of SF 707. 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.

(e) The national stock number of the SF 707 is 7540–01–207–5537.

[52 FR 10190, Mar. 30, 1987]
Information Security Oversight Office, NARA

§ 2003.29 CONFIDENTIAL Label SF 708.

(a) SF 708 is used to identify and protect automatic data processing (ADP) media and other media that contain CONFIDENTIAL information. SF 708 is used instead of the SF 705 for media other than documents.

(b) SF 708 shall be used in all situations that call for the use of a CONFIDENTIAL Label. Agency-wide use of SF 708 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) 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.

(d) Only the Director of ISOO may grant a waiver from the use of SF 708. 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.

(e) The national stock number of the SF 709 is 7540-01-207-5538.

[52 FR 10190, Mar. 30, 1987]

§ 2003.30 CLASSIFIED Label SF 709.

(a) SF 709 is used to identify and protect automatic data processing (ADP) media and other media that contain classified information pending a determination by the classifier of the specific classification level of the information.

(b) SF 709 shall be used in all situations that require the use of a CLASSIFIED Label. Agency-wide use of SF 709 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) 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 SF 706, SF 707, or SF 708 shall be affixed on top of SF 709 so that only the SF 706, SF 707, or SF 708 is visible.

(d) Only the Director of ISOO may grant a waiver from the use of SF 709. 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.

(e) The national stock number of the SF 709 is 7540-01-207-5540.

[52 FR 10190, Mar. 30, 1987]

§ 2003.31 UNCLASSIFIED Label SF 710.

(a) In a mixed environment in which classified and unclassified information are being processed or stored, SF 710 is used to identify automatic data processing (ADP) 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.

(b) SF 710 shall be used in all situations that require the use of an UNCLASSIFIED Label. Agency-wide use of SF 710 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) 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.

(d) Only the Director of ISOO may grant a waiver from the use of SF 710. 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.

(e) The national stock number of the SF 710 is 7540-01-207-5539.

[52 FR 10191, Mar. 30, 1987]
§ 2003.32 DATA DESCRIPTOR Label
SF 711.

(a) SF 711 is used to identify additional safeguarding controls that pertain to classified information that is stored or contained on automatic data processing (ADP) or other media.

(b) SF 711 shall be used in all situations that require the use of a DATA DESCRIPTOR Label. Agency-wide use of SF 711 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) SF 711 is affixed to the ADP medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. 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.

(d) Only the Director of ISOO may grant a waiver from the use of SF 711. 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.

(e) The national stock number of the SF 711 is 7540–01–207–5541.

[52 FR 10191, Mar. 30, 1987]

PART 2004—DIRECTIVE ON SAFE-GUARDING CLASSIFIED NATIONAL SECURITY INFORMATION

§ 2004.1 Authority.

This Directive is issued pursuant to Section 5.2 (c) of Executive Order (E.O.) 12958, “Classified National Security Information.” The E.O. and this Directive set forth the requirements for the safeguarding of classified national security information (hereinafter classified information) and are applicable to all U.S. Government agencies.

§ 2004.2 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 NATO and other foreign government information, agency heads or their designee(s) (hereinafter referred to as agency heads) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director, Information Security Oversight Office (ISOO), to facilitate that office’s oversight responsibility. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasures benefits versus cost.

(c) NATO classified information shall be safeguarded in compliance with U.S.
Information Security Oversight Office, NARA

§ 2004.5

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

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

§ 2004.3 Definitions.

(a) Open storage area. An area, constructed in accordance with Appendix A and authorized by the agency head for open storage of classified information.

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

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

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

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

§ 2004.4 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.

§ 2004.5 Standards for security equipment.

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.
§ 2004.6 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 by one of the following methods:

(i) In a GSA-approved security container with one of the following supplemental controls:
(A) Continuous protection by cleared guard or duty personnel;
(B) Inspection of the security container every two hours by cleared guard or duty personnel;
(C) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or
(D) Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

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

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

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

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

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

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

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

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

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

(3) An IDS (per paragraph (b)(1)(i)(C) of this section) with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

[In addition to one of these supplemental controls specified in paragraphs (b)(2)(iii)(B)(1) through (3), security-in-depth as determined by the agency head is required as part of the supplemental controls for a non-GSA approved container or open storage area storing Secret information.]

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

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

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

(i) Whenever such equipment is placed into use;
(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or
(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the built-in combination lock shall be reset to a standard combination.

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

§ 2004.7 Information controls.

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

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

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

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

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

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

§ 2004.8 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
§2004.8 32 CFR Ch. XX (7–1–01 Edition)

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. An exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a high security padlock, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

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

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

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

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

(ii) Agency heads may, on an exceptional basis and when an urgent requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the General Services Administration contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (39 CFR chapter I) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of classified information. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

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

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

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

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

§ 2004.9 Destruction.

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

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

§ 2004.10 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 government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

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

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

(1) The Department of Justice, and

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

§ 2004.11 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 4.4 of E.O.
§ 2004.12 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 Index of National Security Telecommunications and Information Systems Security Issuances (NSTISSI) and Director of Central Intelligence Directive (DCID) 6/3.


Based upon the risk management factors referenced in §2004.2 of this directive agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures (TSCM) and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, entitled Tempest Countermeasures for Facilities, and SPB Issuance 6-97, entitled National Policy on Technical Surveillance Countermeasures.


Agency heads may prescribe special provisions for the dissemination, transmission, destruction, and safeguarding of classified information during military operations or other emergency situations.

APPENDIX A TO PART 2004—OPEN STORAGE AREAS

This Appendix describes the construction standards for open storage areas.

1. 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.

2. 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.

3. 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 sound baffles, or an intrusion detection system.

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

APPENDIX B TO PART 2004—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, or other obligation. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I-69 and I-70. To the extent practical,
and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government.

1. **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.

2. **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.

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

4. **Restricted and other foreign government information provided in confidence.** In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government “Restricted,” “Designated,” or unclassified provided in confidence), such information must be classified under E.O. 12669. 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 US CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for US CONFIDENTIAL information, the following requirements shall be met:

   a. 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 US (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;

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

   c. 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;

   d. Documents shall be stored in such a manner so as to prevent unauthorized access;

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

5. **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.