in the records will be required, and the position and security clearances or security approvals held by the requester.

(b) *Special procedures.* The Coordinator shall review the request and solicit input from the Director of the Center for the Study of Intelligence and other interested parties concerning whether or not the required determinations set forth in paragraph (c) of this section can be made. After considering any input received, the Coordinator will either make or not make the determinations set forth in paragraph (c), in consultation with the ARP, and forward the request and the Coordinator's recommendation to the Chief, Information Review and Release Group (IRRG), Information Management Services for decision on whether or not to provide the access requested. A negative determination by the Chief of IRRG shall be reviewed by the Director, Information Management Services, who shall issue the final CIA decision whether or not to grant the request for access.

(c) *Determinations.* As a condition precedent for access, the Coordinator must make all of the following determinations with respect to each request:

(1) That the requester is a current staff employee or contractor of the U.S. Government;

(2) That the requester is currently cleared, or security approved, for access to classified information and that the specific clearance or security approval and access levels of that individual has been officially recorded;

(3) That the scope of the request for information is clearly delineated;

(4) That the information requested is reasonably accessible and can be located and compiled with a reasonable effort;

(5) That a nondisclosure agreement with a prepublication review clause has been executed by the requester;

(6) That all notes and any resulting document will be appropriately safeguarded, that further access will be appropriately limited, and that no further dissemination of information such as that marked ORCON (Dissemination and Extraction of Information Controlled by Originator) or HUMINT (Human Intelligence) shall be made beyond the requesting agency unless CIA permission is obtained;

(7) That if the resulting document containing CIA information or equities is intended to be declassified, the document will be submitted to the Coordinator for declassification review;

(8) That the information and documents will remain classified until a final declassification review and release decision is made by CIA; and,

(9) That the request for access is an official agency request, made in the requester's official capacity on behalf of the requester's agency.

(d) *Limitations.* (1) With respect to requests for access to CIA information and equities residing outside of CIA, upon a favorable CIA determination in accordance with paragraph (c) of this section, the CIA will notify both the requester and the agency holding the records with CIA equities. The requester will need to follow the access requirements of the agency holding the records in addition to any access requirements mandated by CIA.

(2) If access to classified historical CIA records is granted, as a rule, such access shall be provided on CIA premises only. No copies of any classified historical CIA records shall be provided to the requester for reference and use on requester premises without the express approval of the Director, Information Management Services. In exceptional cases, if the provision of classified CIA historical records to the requester for reference and use on requester premises is permitted, the classified CIA historical records provided shall not be disclosed or disseminated beyond the requesting agency, and shall be returned to CIA or destroyed when use of the records has ended. Similarly, any notes taken that are derived from classified historical CIA records that have been accessed in accordance with this part shall not be disclosed or disseminated beyond the requesting agency.

PARTS 1912–1999 [RESERVED]

CHAPTER XX—INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

PART 2000—ADMINISTRATIVE PROCEDURES [RESERVED]

PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION

Subpart A—Scope of Part

Subpart B—Classification

Subpart C—Identification and Markings

Subpart D—Declassification

Subpart E—Safeguarding

Subpart F—Self-Inspections

Subpart G—Security Education and Training

Subpart H—Standard Forms

Subpart I—Reporting and Definitions

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

SOURCE: 75 FR 37254, June 28, 2010, unless otherwise noted.

Subpart A—Scope of Part

§ 2001.1 Purpose and scope.

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

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

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

CFR section	Related section of E.O. 13526
2001.10 Classification standards	1.1, 1.4

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

Subpart B—Classification

§ 2001.10 Classification standards.

Identifying or describing damage to the national security. Section 1.1(a) of the Order specifies the conditions that must be met when making classification decisions. Section 1.4 specifies that information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand pursuant to the Order or law.

§ 2001.11 Original classification authority.

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

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

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

§ 2001.12 Duration of classification.

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

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

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

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

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

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

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

(b) *Extending duration of classification for information classified under the Order.* Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

(1) If the date or event assigned by the original classification authority has not passed, an original classification authority with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origin of the record.

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

(3) In all cases, when extending the duration of classification, the original classification authority must:

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

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

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

(c) *Duration of information classified under prior orders*—(1) *Specific date or event.* Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. If the specific date or event has not passed, an original classification authority with jurisdiction over the information may extend the duration in accordance with the requirements of paragraph (b) of this section. If the date or event assigned by the original classification authority has passed, an original classification authority with jurisdiction over the information may only reclassify information in accordance with

the standards and procedures under the Order and this Directive. If the information is contained in records determined to be permanently valuable, and the prescribed date or event will take place more than 25 years from the date of origin of the document, the declassification of the information will instead be subject to section 3.3 of the Order.

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

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

(ii) An original classification authority with jurisdiction over the information may re-mark the information to establish a duration of classification of no more than 25 years from the date of origin of the document, consistent with the requirements for information originally classified under the Order, as provided in paragraph (a) of this section; or

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

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

§ 2001.13 Classification prohibitions and limitations.

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

(1) If the information at issue is in records in the physical and legal custody of the National Archives and Records Administration (NARA) and has been made available to the public, the original classification authority with jurisdiction over the information shall, as part of determining whether the restoration of markings and controls is appropriate, consider whether the removal of the information from public purview will significantly mitigate the harm to national security or otherwise draw undue attention to the information at issue. Written notification, classified when appropriate under the Order, shall be made to the Archivist, which shall include a description of the record(s) at issue, the elements of information that are classified, the duration of classification, and the specific authority for continued classification. If the information at issue is more than 25 years of age and the Archivist does not agree with the decision, the information shall nonetheless be temporarily withdrawn from public access and shall be referred to the Director of ISOO for resolution in collaboration with affected parties.

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

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

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

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

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

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

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

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

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

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

§ 2001.14 Classification challenges.

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

(b) *Agency procedures.* (1) Because the Order encourages authorized holders to challenge classification as a means for promoting proper and thoughtful classification actions, agencies shall ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

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

(3) The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond to the challenge within 60

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

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

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

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

§ 2001.15 Classification guides.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) Originators of classification guides are encouraged to consult the

users of guides and other subject matter experts when reviewing or updating guides. Also, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide.

§ 2001.16 Fundamental classification guidance review.

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

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

(1) Evaluation of content.

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

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

(2) Evaluation of use:

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

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

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

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

Subpart C—Identification and Markings

§ 2001.20 General.

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

§ 2001.21 Original classification.

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

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

Classified By: David Smith, Chief, Division 5

or

Classified By: ID#IMNO1

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

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

(3) *Reason for classification.* The original classification authority shall identify the reason(s) for the decision to classify. The original classification authority shall include on the ''Reason'' line the number 1.4 plus the letter(s) that corresponds to that classification category in section 1.4 of the Order.

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

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

(B) Foreign government information;

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

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

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

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

(G) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(H) The development, production, or use of weapons of mass destruction.

(ii) An example might appear as:

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

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

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

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

(ii) A date not to exceed 25 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2010, apply a date up to 25 years on the ''Declassify On'' line:

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

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

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

(b) *Overall marking.* The highest level of classification is determined by the highest level of any one portion within the document and shall appear in a way that will distinguish it clearly from the informational text.

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

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

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

(c) *Portion marking.* Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks,

bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies.

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

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

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

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

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

§ 2001.22 Derivative classification.

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

(b) *Identity of persons who apply derivative classification markings.* Derivative classifiers shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin shall be identified and follow the name on the ''Classified By'' line. An example might appear as:

Classified By: Peggy Jones, Lead Analyst, Research and Analysis Division or
Classified By: ID # IMN01

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

Derived From: Memo, ''Funding Problems,'' October 20, 2008, Office of Administration, Department of Good Works or
Derived From: CG No. 1, Department of Good Works, dated October 20, 2008

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

Derived From: Multiple Sources

(ii) The derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document.

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

Derived From: Report entitled, ''New Weapons,'' dated October 20, 2009, Department of Good Works, Office of Administration

(d) *Reason for classification.* The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not transferred in a derivative classification action.

(e) *Declassification instructions.* (1) The derivative classifier shall carry forward the instructions on the ''Declassify On'' line from the source document to the derivative document, or the duration instruction from the classification or declassification guide, unless it contains one of the declassification instructions as listed in paragraph (e)(3) of this section. If the source document is missing the declassification instruction, then a calculated date of 25 years from the date of the source document (if available) or the current date (if the source document date is not available) shall be carried forward by the derivative classifier.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 2001.23 Classification marking in the electronic environment.

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

(1) Subject to all requirements of the Order.

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

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

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

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

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

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

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

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

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

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

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

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

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

(4) Classified Web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion.

A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

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

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

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

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

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

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

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

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

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

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

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

(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the

subject line itself, not the content of the post.

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

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

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

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

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

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

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

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

(ii) *Reserved.*

§ 2001.24 Additional requirements.

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

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

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

(c) *Foreign government information.* Unless otherwise evident, documents that contain foreign government information should include the marking, ''This Document Contains (indicate country of origin) Information.'' Agencies may also require that the portions of the documents that contain the foreign government information be marked to indicate the government and classification level, using accepted country code standards, *e.g.*, ''(Country code—C).'' If the identity of the specific government must be concealed, the document shall be marked, ''This Document Contains Foreign Government Information,'' and pertinent portions shall be marked ''FGI'' together with the classification level, *e.g.*, ''(FGI–C).'' In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. If the fact that information is foreign government information must be concealed, the markings described in this paragraph shall not be

used and the document shall be marked as if it were wholly of U.S. origin. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information.

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

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

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

(3) Filed permanently.

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

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

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

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

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

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

(4) If an RD or FRD portion is extracted for use in a new document, the

requirements of 10 CFR part 1045 must be followed.

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

(6) If a commingled document is not portion marked based on appropriate authority, annotating the source list with the declassification instructions and including the ''Declassify on'' line in accordance with paragraph (h)(3) of this section are not required. The lack of declassification instructions does not eliminate the requirement to process commingled documents for declassification in accordance with the Order, this Directive, the Atomic Energy Act, or 10 CFR part 1045 when they are requested under statute or the Order.

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

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

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

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

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

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

(k) *Portion marking waivers.* (1) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information. Such a request shall be submitted to the Director of ISOO and should include the reasons that the benefits of portion marking are outweighed by other factors. The request must also demonstrate that the requested waiver will not create impediments to information sharing. Statements citing administrative burden alone will ordinarily not be viewed

as sufficient grounds to support a waiver.

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

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

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

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

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

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

(i) The level of classification;

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

(iii) Declassification instructions;

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

(v) The date the reclassification action was taken.

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

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

§ 2001.25 Declassification markings.

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

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

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

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

(3) The date of declassification; and

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

~~SECRET~~
Declassified by David Smith, Chief, Division 5, August 17, 2008

§ 2001.26 Automatic declassification exemption markings.

(a) *Marking information exempted from automatic declassification at 25 years.* (1) When the Panel has approved an agency proposal to exempt permanently valuable information from automatic

declassification at 25 years, the ''Declassify On'' line shall be revised to include the symbol ''25X'' plus the number(s) that corresponds to the category(ies) in section 3.3(b) of the Order. Except for when the exemption pertains to information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, or a human intelligence source, or key design concepts of weapons of mass destruction, the revised ''Declassify On'' line shall also include the new date for declassification as approved by the Panel, not to exceed 50 years from the date of origin of the record. Records that contain information, the release of which should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, are exempt from automatic declassification at 50 years.

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

25X1: reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

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

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

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

25X5: reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

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

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

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

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

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

Declassify On: 25X4, 20501001

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

(5) Agencies need not apply a ''25X'' marking to individual documents contained in a file series exempted from automatic declassification under section 3.3(c) of the Order until the individual document is removed from the file and may only apply such a marking as approved by the Panel under section 3.3(j) of the Order.

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

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

(1) When the information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence

source, the marking shall be ''50X1–HUM.''

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

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

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

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

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

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

Subpart D—Declassification

§ 2001.30 Automatic declassification.

(a) *General.* All departments and agencies that have original classification authority or previously had original classification authority, or maintain records determined to be permanently valuable that contain classified national security information, shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in managing automatic declassification of accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist.

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

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

(d) *Transferred information.* In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage,

the receiving agency shall be deemed to be the originating agency.

(e) *Unofficially transferred information.* In the case of classified information that is not officially transferred as described in paragraph (d) of this section but that originated in an agency that has ceased to exist and for which there is no successor agency, the agency in possession shall serve as the originating agency and shall be responsible for actions for those records in accordance with section 3.3 of the Order and in consultation with the Director of the National Declassification Center (NDC).

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

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

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

(i) *Foreign government information.* The declassifying agency is the agency that initially received or classified the information. When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency shall also determine if another exemption under section 3.3(b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government prior to declassification.

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

(k) *Use of approved declassification guides.* Approved declassification guides are the sole basis for the exemption from automatic declassification of specific information as provided in section 3.3(b) of the Order and the sole basis for the continued classification of information under section 3.3(h) of the Order. These guides must be prepared in accordance with section 3.3(j) of the Order and include additional pertinent detail relating to the exemptions described in sections 3.3(b) and 3.3(h) of the Order, and follow the format required of declassification guides as described in § 2001.32. During a review

under section 3.3 of the Order, it is expected that agencies will use these guides to identify specific information for exemption from automatic declassification. It is further expected that the guides or detailed declassification guidance will be made available to the NDC under section 3.7(b) of the Order and to appropriately cleared individuals of other agencies to support equity recognition.

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

(m) *Exemption from Automatic Declassification at 25, 50, or 75 years.* Agencies may propose to exempt from automatic declassification specific information, either by reference to information in specific records, in specific file series of records, or in the form of a declassification guide, in accordance with section 3.3(j) of the Order. Agencies may propose to exempt information within five years of, but not later than one year before the information is subject to automatic declassification. The agency head or senior agency official, within the specified timeframe, shall notify the Director of ISOO, serving as the Executive Secretary of the Panel, of the specific information being proposed for exemption from automatic declassification.

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

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

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

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

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

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

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

(3) *Newly discovered records.* An agency head or senior agency official must consult with the Director of ISOO on any decision to delay automatic declassification of newly discovered records no later than 90 days, from the

discovery of the records. The notification shall identify the records, their volume, the anticipated date for declassification, and the circumstances of the discovery. An agency may be granted up to three years from the date of discovery to make a declassification, exemption, or referral determination. If referrals to other agencies are properly identified, they will be handled in accordance with subparagraphs 2(i) and 2(ii) above.

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

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

(o) *Redaction standard.* Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.3 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

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

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

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

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

(2) Formerly Restricted Data is information that is still classified under the Atomic Energy Act of 1954, as amended, but which has been removed from the Restricted Data category because it is related primarily to the military utilization of atomic weapons.

(3) Any document marked as containing Restricted Data or Formerly Restricted Data or identified as potentially containing unmarked Restricted Data or Formerly Restricted Data shall be referred to the Department of Energy in accordance with § 2001.34(b)(8).

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

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

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

§ 2001.31 Systematic declassification review.

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

§ 2001.32 Declassification guides.

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

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

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

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

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

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

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

(i) The appropriate exemption category listed in section 3.3(b), and, if appropriate, section 3.3(h) of the Order; and

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

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

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

(2) Declassification guides or detailed declassification guidance shall be submitted to the Director of the NDC in

accordance with section 3.7(b)(3) of the Order.

§ 2001.33 Mandatory review for declassification.

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

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

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall promptly process the request for declassification and release in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency. The referring agency is responsible for collecting all agency review results and informing the requestor of any final decision regarding the declassification of the requested information unless a prior arrangement has been made with the originating agency.

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

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

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

(b) *Foreign government information.* Except as provided in this paragraph, agencies shall process mandatory declassification review requests for classified records containing foreign government information in accordance with this section. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

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

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

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

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

(g) *FOIA and Privacy Act requests.* Agency heads shall process requests for declassification that are submitted under the provisions of the FOIA, as amended, or the Privacy Act of 1974 (5 U.S.C. 552a), as amended, in accordance with the provisions of those Acts.

(h) *Redaction standard.* Agencies shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction. The specific reason for the redaction, as provided for in section 1.4 or 3.3(b) of the Order, as applicable, must be included for each redaction. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction. Any such redactions shall be performed in accordance with policies and procedures established in accordance with § 2001.45(d).

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

§ 2001.34 Referrals.

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

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

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

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

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

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

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

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

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

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

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

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

(9) The NDC, as well as any centralized agency facility established under section 3.7(e) of the Order, shall track

and document referral actions and decisions in a manner that facilitates archival processing for public access. Central agency facilities must work with the NDC to ensure documentation meets NDC requirements, and transfer all documentation on pending referral actions and referral decisions to the NDC when transferring the records to NARA.

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

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

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

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

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

§ 2001.35 Discretionary declassification.

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

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

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

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

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

§ 2001.37 Assistance to the Department of State.

Heads of agencies shall assist the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by facilitating access to appropriate classified materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS. If an agency fails to provide a final declassification review determination regarding a Department of State referral within 120 days of the date of the referral, or if applicable, within 120 days of the date of a High Level Panel decision, the Department of State, consistent with 22 U.S.C. 4353 and any implementing agency procedures, may seek the assistance of the Panel.

Subpart E—Safeguarding

§ 2001.40 General.

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

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

(c) North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instruction (USSAN) 1–07. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at § 2001.54 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) *Need-to-know determinations.* (1) Agency heads, through their designees, shall identify organizational missions and personnel requiring access to classified information to perform or assist in authorized governmental functions. These mission and personnel requirements are determined by the functions of an agency or the roles and responsibilities of personnel in the course of their official duties. Personnel determinations shall be consistent with section 4.1(a) of the Order.

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

§ 2001.41 Responsibilities of holders.

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

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

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

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

§ 2001.42 Standards for security equipment.

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

standards and specifications established by the Administrator of the GSA, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

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

§ 2001.43 Storage.

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

(b) *Requirements for physical protection*—(1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with §2001.53. In addition, supplemental controls are required as follows:

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

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

(B) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation. Acceptability of Intrusion Detection Equipment (IDE): All IDE must be in accordance with standards approved by ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head; or

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

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

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

(2) *Secret.* Secret information shall be stored in the same manner as Top Secret information or, until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock. Security-In-Depth is required in areas in which a non-GSA-approved container or open storage area is located. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required:

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

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

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

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

(1) *Equipment in service.* Combinations to dial-type locks shall be changed only by persons authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(i) Whenever such equipment is placed into use;

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

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

(2) *Equipment out of service.* When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the combination lock should be reset to a standard combination of 50–25–50 for built-in combination locks or 10–20–30 for combination padlocks.

(d) *Key operated locks.* When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be included in implementing regulations required under section 5.4(d)(2) of the Order.

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

§ 2001.44 Reciprocity of use and inspection of facilities.

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

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

§ 2001.45 Information controls.

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

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

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

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

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

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

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

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

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

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

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

§ 2001.46 Transmission.

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

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

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

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

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

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

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

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

(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on

direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF–P–110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(c) *Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory*—(1) *Top Secret.* Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other cleared or uncleared commercial carrier.

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

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

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

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

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

(e) *Transmission of U.S. classified information to foreign governments.* Such transmission shall take place between designated government representatives using the government-to-government transmission methods described in paragraph (d) of this section or through channels agreed to by the National Security Authorities of the two governments. When classified information is transferred to a foreign government or

its representative a signed receipt is required.

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

§ 2001.47 Destruction.

Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Agencies shall comply with the destruction equipment standard stated in § 2001.42(b) of this Directive.

§ 2001.48 Loss, possible compromise or unauthorized disclosure.

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

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

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

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

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

(2) May attract significant public attention;

(3) Involves large amounts of classified information; or

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

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

(1) The Department of Justice, and

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

§ 2001.49 Special access programs.

(a) *General.* The safeguarding requirements of this Directive may be enhanced for information in special access programs (SAP), established under the provisions of section 4.3 of the Order by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

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

§ 2001.50 Telecommunications automated information systems and network security.

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation.*

§ 2001.51 Technical security.

Based upon the risk management factors referenced in § 2001.40 of this directive, agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, *TEMPEST Countermeasures for Facilities,* and SPB Issuance 6–97, *National Policy on Technical Surveillance Countermeasures.*

§ 2001.52 Emergency authority.

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

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

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

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

(3) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in § 2001.46, or other means deemed necessary when time is of the essence;

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

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

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

(i) A description of the disclosed information;

(ii) To whom the information was disclosed;

(iii) How the information was disclosed and transmitted;

(iv) Reason for the emergency release;

(v) How the information is being safeguarded; and

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

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

§ 2001.53 Open storage areas.

This section describes the minimum construction standards for open storage areas.

(a) *Construction.* The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in

a manner as to provide visual evidence of unauthorized penetration.

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

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

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

(2) Windows within 18 feet of the ground will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

§ 2001.54 Foreign government information.

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation. NATO classified information shall be safeguarded in compliance with USSAN 1–07. To the extent practical, and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described in paragraphs (a) through (e) of this section may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government, hereafter ''originating government.''

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

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

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

(d) *Restricted and other foreign government information provided in confidence.* In order to assure the protection of other foreign government information provided in confidence (*e.g.*, foreign government ''Restricted,'' ''Designated,'' or unclassified provided in confidence), such information must be classified under the Order. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that

required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements shall be met:

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

(2) Documents shall be provided only to persons in accordance with sections 4.1(a) and (h) of the Order;

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

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

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

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

§ 2001.55 Foreign disclosure of classified information.

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

Subpart F—Self-Inspections

§ 2001.60 General.

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

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

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

(1) Self-inspections should evaluate the adherence to the principles and requirements of the Order and this directive and the effectiveness of agency

programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

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

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

(d) *Frequency.* Self-inspections shall be regular, ongoing, and conducted at least annually with the senior agency official setting the frequency on the basis of program needs and the degree of classification activity. Activities that generate significant amounts of classified information shall include a representative sample of their original and derivative classification actions.

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

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

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

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

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

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

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

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

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

Subpart G—Security Education and Training

§ 2001.70 General.

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

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

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

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

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

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

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

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

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

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

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

§ 2001.71 Coverage.

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

(b) *Initial training.* All cleared agency personnel shall receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. Such training must be provided in conjunction with the granting of a security clearance, and prior to accessing classified information.

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

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

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

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

(i) An agency head, deputy agency head, or senior agency official may grant a waiver of this requirement if an individual is unable to receive this

training due to unavoidable circumstances. All such waivers shall be documented.

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

(d) *Training for persons who apply derivative classification markings.* Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the Order, emphasizing the avoidance of overclassification. At a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

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

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

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

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

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

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

(f) *Annual refresher security education and training.* Agencies shall provide annual refresher training to employees who create, process, or handle classified information. Annual refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Annual refresher training should also address identification and handling of other agency-originated information and foreign government information, as well as the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Annual refresher training should also address issues or concerns identified during agency self-inspections.

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

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

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

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

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

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

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

Subpart H—Standard Forms

§ 2001.80 Prescribed standard forms.

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

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

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

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

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

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

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

(ii) The SF 312 may be filled out electronically or by hand, then must be signed. It may be signed by hand and scanned, if the implementing agency permits and the scanned version is done in a way that constitutes a legally enforceable facsimile. Alternatively, the form may be digitally signed if the implementing agency permits, and if the digital signature mechanism employs public key cryptography in a way that meaningfully guarantees authenticity (*i.e.*, that the digital signature was made by the person it claims to have been made by); consent (*i.e.*, that the person who digitally signed the form meant to do so); and integrity (*i.e.*, that the SF 312 has not changed since the signature was made). Digital signatures created using Personal Identity Verification (PIV) cards or common access cards (CACs) issued by the U.S. Government that are compliant with Homeland Security Presidential Directive 12 (HSPD–12), or its successor, meet the requirements of this paragraph (d)(2)(ii). They include public key infrastructure (PKI), digital signature certificates issued by a certificate authority (CA), and a PIN the signer must enter in order to digitally sign. Agencies may choose to use other digital signature mechanisms than the PIV or CAC cards, as long as they meet the requirements of this paragraph (d)(2)(ii). The form may not be signed using other forms of electronic signature (e-signature), such as typing ''/s/

[first and last name]'' or attaching an image of a handwritten signature.

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

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

(v) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee, or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States. If the SF 312 is digitally signed, it does not require a witness to observe and verify the digital signature, and therefore also does not require an official to subsequently accept the signature.

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

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

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

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

(3) *SF 700, Security Container Information:* The SF 700 provides the names, addresses, and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended. The form also includes the means to maintain a current record of the security container's combination and provides the envelope to be used to

forward this information to the appropriate agency activity or official. If an agency determines, as part of its risk management strategy, that a security container information form is required, the SF 700 shall be used. Parts 2 and 2A of each completed copy of SF 700 shall be classified at the highest level of classification of the information authorized for storage in the security container. A new SF 700 must be completed each time the combination to the security container is changed. The national stock number for the SF 700 is 7540–01–214–5372.

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

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

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

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

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

(9) *SF 706, TOP SECRET Label:* The SF 706 is used to identify and protect electronic media and other media that contain Top Secret information. The SF 706 is used instead of the SF 703 for media other than documents. If an agency determines, as part of its risk management strategy, that a TOP SECRET label is required, the SF 706 will be used. The SF 706 is affixed to the medium containing Top Secret information in a manner that would not adversely affect operation of equipment in which the medium is used. Once the label has been applied, it cannot be removed. The national stock number of the SF 706 is 7540–01–207–5536.

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

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

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

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

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

(15) *SF 714, Financial Disclosure Report:* When required by an agency head or by the Director of National Intelligence, as the Security Executive Agent, the SF 714 contains information that is used to make personnel security determinations, including whether to grant a security clearance; to allow access to classified information, sensitive areas, and equipment; or to permit assignment to sensitive national security

positions. The data may later be used as a part of a review process to evaluate continued eligibility for access to classified information or as evidence in legal proceedings. The SF 714 assists law enforcement agencies in obtaining pertinent information in the preliminary stages of potential espionage and counter terrorism cases.

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

[75 FR 37254, June 28, 2010, as amended at 87 FR 17952, Mar. 29, 2022]

Subpart I—Reporting and Definitions

§ 2001.90 Agency annual reporting requirements.

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

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

(c) *Accounting for costs*. (1) Information on the costs associated with the implementation of the Order will be collected from the agencies. The agencies will provide data to ISOO on the cost estimates for classification-related activities. ISOO will report these cost estimates annually to the President. The agency senior official should work closely with the agency comptroller to ensure that the best estimates are collected.

(2) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O.12829, as amended, *National Industrial Security Program*, and consistent with agreements entered into under section 202 of E.O. 12989, as amended, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will report these cost estimates annually to the President.

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

§ 2001.91 Other agency reporting requirements.

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

(b) *Reclassification actions*. Reclassification of information that has been declassified and released under proper authority shall be reported promptly to the National Security Advisor and the Director of ISOO in accordance with section 1.7(c)(3) of the Order and § 2001.13(b).

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

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

§ 2001.92 Definitions.

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

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

(c) *Classification management* means the life-cycle management of classified national security information from

original classification to declassification.

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

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

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

(g) *Equity* refers to information:

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

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

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

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

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

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

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

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

(m) *Original classification authority with jurisdiction over the information* includes:

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

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

(3) A supervisory official of either; or

(4) The senior agency official under the Order.

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

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

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

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

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

(p) *Presidential papers, historical materials, and records* means the papers or records of the former Presidents under

the legal control of the Archivist pursuant to sections 2111, 2111 note, or 2203 of title 44, U.S.C.

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

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

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

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

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

(v) *Transclassification* means information that has been removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive orders as ''National Security Information.''

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

PART 2002—CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Subpart A—General Information

Subpart B—Key Elements of the CUI Program

Subpart C—CUI Program Management

AUTHORITY: E.O. 13556, 75 FR 68675, 3 CFR, 2010 Comp., pp. 267–270.

SOURCE: 81 FR 63336, Sept. 14, 2016, unless otherwise noted.

Subpart A—General Information

§ 2002.1 Purpose and scope.

(a) This part describes the executive branch's Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI.

(b) The CUI Program standardizes the way the executive branch handles information that requires protection

under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526, Classified National Security Information, December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, *et seq.*), as amended.

(c) All unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI. Law, regulation (to include this part), or Government-wide policy must require or permit such controls. Agencies therefore may not implement safeguarding or dissemination controls for any unclassified information other than those controls consistent with the CUI Program.

(d) Prior to the CUI Program, agencies often employed *ad hoc*, agency-specific policies, procedures, and markings to handle this information. This patchwork approach caused agencies to mark and handle information inconsistently, implement unclear or unnecessarily restrictive disseminating policies, and create obstacles to sharing information.

(e) An executive branch-wide CUI policy balances the need to safeguard CUI with the public interest in sharing information appropriately and without unnecessary burdens.

(f) This part applies to all executive branch agencies that designate or handle information that meets the standards for CUI. This part does not apply directly to non-executive branch entities, but it does apply indirectly to non-executive branch CUI recipients, through incorporation into agreements (see §§ 2002.4(c) and 2002.16(a) for more information).

(g) This part rescinds Controlled Unclassified Information (CUI) Office Notice 2011–01: Initial Implementation Guidance for Executive Order 13556 (June 9, 2011).

(h) This part creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(i) This part, which contains the CUI Executive Agent (EA)'s control policy, overrides agency-specific or *ad hoc* requirements when they conflict. This part does not alter, limit, or supersede a requirement stated in laws, regulations, or Government-wide policies or impede the statutory authority of agency heads.

§ 2002.2 Incorporation by reference.

(a) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, NARA must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. You may inspect all approved material incorporated by reference at NARA's textual research room, located at National Archives and Records Administration; 8601 Adelphi Road; Room 2000; College Park, MD 20740–6001. To arrange to inspect this approved material at NARA, contact NARA's Regulation Comments Desk (Strategy and Performance Division (SP)) by email at *regulation_comments@nara.gov* or by telephone at 301.837.3151. All approved material is available from the sources listed below. You may also inspect approved material at the Office of the Federal Register (OFR). For information on the availability of this material at the OFR, call 202–741–6030 or go to *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*.

(b) The National Institute of Standards and Technology (NIST), by mail at 100 Bureau Drive, Stop 1070; Gaithersburg, MD 20899–1070, by email at *inquiries@nist.gov*, by phone at (301) 975–NIST (6478) or Federal Relay Service (800) 877–8339 (TTY), or online at *http://nist.gov/publication-portal.cfm*.

(1) FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004. IBR approved for §§ 2002.14(c) and (g), and 2002.16(c).

(2) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. IBR approved for §§ 2002.14(c) and (g), and 2002.16(c).

(3) NIST Special Publication 800–53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (includes updates as of 01–22–2015), (NIST SP 800–53). IBR approved for §§ 2002.14(c), (e), (f), and (g), and 2002.16(c).

(4) NIST Special Publication 800–88, Guidelines for Media Sanitization, Revision 1, December 2014, (NIST SP 800–88). IBR approved for § 2002.14(f).

(5) NIST Special Publication 800–171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, June 2015 (includes updates as of January 14, 2016), (NIST SP 800–171). IBR approved for § 2002.14(h).

§ 2002.4 Definitions.

As used in this part:

(a) *Agency* (also Federal agency, executive agency, executive branch agency) is any ''executive agency,'' as defined in 5 U.S.C. 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

(b) *Agency CUI policies* are the policies the agency enacts to implement the CUI Program within the agency. They must be in accordance with the Order, this part, and the CUI Registry and approved by the CUI EA.

(c) *Agreements and arrangements* are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreements or arrangements that include CUI provisions whenever feasible (see § 2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see § 2002.16(a)(5)(iii) and (a)(6) for details).

(d) *Authorized holder* is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part.

(e) *Classified information* is information that Executive Order 13526, ''Classified National Security Information,'' December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.

(f) *Controlled environment* is any area or space an authorized holder deems to have adequate physical or procedural controls (*e.g.*, barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

(g) *Control level* is a general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

(h) *Controlled Unclassified Information* (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

(i) *Controls* are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may

specify the controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case, the agency applies controls from the Order, this part, and the CUI Registry).

(j) *CUI Basic* is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified in this section), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

(k) *CUI categories and subcategories* are those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the CUI Registry. The controls for any CUI Basic categories and any CUI Basic subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic ones and from each other. A CUI category may be Specified, while some or all of its subcategories may not be, and vice versa. If dealing with CUI that falls into a CUI Specified category or subcategory, review the controls for that category or subcategory on the CUI Registry. Also consult the agency's CUI policy for specific direction from the Senior Agency Official.

(l) *CUI category or subcategory markings* are the markings approved by the CUI EA for the categories and subcategories listed in the CUI Registry.

(m) *CUI Executive Agent (EA)* is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

(n) *CUI Program* is the executive branch-wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI, established by the Order, this part, and the CUI Registry.

(o) *CUI Program manager* is an agency official, designated by the agency head or CUI SAO, to serve as the official representative to the CUI EA on the agency's day-to-day CUI Program operations, both within the agency and in interagency contexts.

(p) *CUI Registry* is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

(q) *CUI senior agency official (SAO)* is a senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. The CUI SAO is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI EA.

(r) *CUI Specified* is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

(s) *Decontrolling* occurs when an authorized holder, consistent with this part and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action. See § 2002.18.

(t) *Designating CUI* occurs when an authorized holder, consistent with this part and the CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with this part.

(u) *Designating agency* is the executive branch agency that designates or approves the designation of a specific item of information as CUI.

(v) *Disseminating* occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external to an agency.

(w) *Document* means any tangible thing which constitutes or contains information, and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.

(x) *Federal information system* is an information system used or operated by an agency or by a contractor of an agency or other organization *on behalf of an agency*. 44 U.S.C. 3554(a)(1)(A)(ii).

(y) *Foreign entity* is a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.

(z) *Formerly Restricted Data (FRD)* is a type of information classified under the Atomic Energy Act, and defined in 10 CFR 1045, Nuclear Classification and Declassification.

(aa) *Handling* is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

(bb) *Lawful Government purpose* is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

(cc) *Legacy material* is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

(dd) *Limited dissemination control* is any CUI EA-approved control that agencies may use to limit or specify CUI dissemination.

(ee) *Misuse of CUI* occurs when someone uses CUI in a manner not in accordance with the policy contained in the Order, this part, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected

information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

(ff) *National Security System* is a special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42 and 44 U.S.C. 3542(b)(2).

(gg) *Non-executive branch entity* is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities as defined in this part, nor does it include individuals or organizations when they receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974.

(hh) *On behalf of an agency* occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

(ii) *Order* is Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267), or any successor order.

(jj) *Portion* is ordinarily a section within a document, and may include subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, bullets points, or other sections.

(kk) *Protection* includes all controls an agency applies or must apply when handling information that qualifies as CUI.

(ll) *Public release* occurs when the agency that originally designated particular information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though an agency may disclose some CUI to a member of the public, the Government must still control that CUI unless the agency publicly releases it through its official public release processes.

(mm) *Records* are agency records and Presidential papers or Presidential records (or Vice-Presidential), as those terms are defined in 44 U.S.C. 3301 and 44 U.S.C. 2201 and 2207. Records also include such items created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.

(nn) *Required or permitted (by a law, regulation, or Government-wide policy)* is the basis by which information may qualify as CUI. If a law, regulation, or Government-wide policy requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as ''is exempt from'' applying certain information release or disclosure requirements, ''may'' release or disclose the information, ''may not be required to'' release or disclose the information, ''is responsible for protecting'' the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

(oo) *Restricted Data (RD)* is a type of information classified under the Atomic Energy Act, defined in 10 CFR part 1045, Nuclear Classification and Declassification.

(pp) *Re-use* means incorporating, restating, or paraphrasing information from its originally designated form into a newly created document.

(qq) *Self-inspection* is an agency's internally managed review and evaluation of its activities to implement the CUI Program.

(rr) *Unauthorized disclosure* occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.

(ss) *Uncontrolled unclassified information* is information that neither the Order nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.

(tt) *Working papers* are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

§ 2002.6 CUI Executive Agent (EA).

(a) Section 2(c) of the Order designates NARA as the CUI Executive Agent (EA) to implement the Order and to oversee agency efforts to comply with the Order, this part, and the CUI Registry.

(b) NARA has delegated the CUI EA responsibilities to the Director of ISOO. Under this authority, ISOO staff carry out CUI oversight responsibilities and manage the Federal CUI program.

§ 2002.8 Roles and responsibilities.

(a) The CUI EA:

(1) Develops and issues policy, guidance, and other materials, as needed, to implement the Order, the CUI Registry, and this part, and to establish and maintain the CUI Program;

(2) Consults with affected agencies, Government-wide policy bodies, State, local, Tribal, and private sector partners, and representatives of the public on matters pertaining to CUI as needed;

(3) Establishes, convenes, and chairs the CUI Advisory Council (the Council) to address matters pertaining to the CUI Program. The CUI EA consults with affected agencies to develop and document the Council's structure and procedures, and submits the details to OMB for approval;

(4) Reviews and approves agency policies implementing this part to ensure their consistency with the Order, this part, and the CUI Registry;

(5) Reviews, evaluates, and oversees agencies' actions to implement the CUI Program, to ensure compliance with the Order, this part, and the CUI Registry;

(6) Establishes a management and planning framework, including associated deadlines for phased implementation, based on agency compliance plans submitted pursuant to section 5(b) of the Order, and in consultation with affected agencies and OMB;

(7) Approves categories and subcategories of CUI as needed and publishes them in the CUI Registry;

(8) Maintains and updates the CUI Registry as needed;

(9) Prescribes standards, procedures, guidance, and instructions for oversight and agency self-inspection programs, to include performing on-site inspections;

(10) Standardizes forms and procedures to implement the CUI Program;

(11) Considers and resolves, as appropriate, disputes, complaints, and suggestions about the CUI Program from entities in or outside the Government; and

(12) Reports to the President on implementation of the Order and the requirements of this part. This includes publishing a report on the status of agency implementation at least biennially, or more frequently at the discretion of the CUI EA.

(b) Agency heads:

(1) Ensure agency senior leadership support, and make adequate resources available to implement, manage, and comply with the CUI Program as administered by the CUI EA;

(2) Designate a CUI senior agency official (SAO) responsible for oversight of

the agency's CUI Program implementation, compliance, and management, and include the official in agency contact listings;

(3) Approve agency policies, as required, to implement the CUI Program; and

(4) Establish and maintain a self-inspection program to ensure the agency complies with the principles and requirements of the Order, this part, and the CUI Registry.

(c) The CUI SAO:

(1) Must be at the Senior Executive Service level or equivalent;

(2) Directs and oversees the agency's CUI Program;

(3) Designates a CUI Program manager;

(4) Ensures the agency has CUI implementing policies and plans, as needed;

(5) Implements an education and training program pursuant to §2002.30;

(6) Upon request of the CUI EA under section 5(c) of the Order, provides an update of CUI implementation efforts for subsequent reporting;

(7) Submits to the CUI EA any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that the agency proposes to use to designate unclassified information for safeguarding or dissemination controls;

(8) Coordinates with the CUI EA, as appropriate, any proposed law, regulation, or Government-wide policy that would establish, eliminate, or modify a category or subcategory of CUI, or change information controls applicable to CUI;

(9) Establishes processes for handling CUI decontrol requests submitted by authorized holders;

(10) Includes a description of all existing waivers in the annual report to the CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps the agency is taking to ensure sufficient protection of CUI within the agency;

(11) Develops and implements the agency's self-inspection program;

(12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for instructions when they receive unmarked or improperly marked information the agency designated as CUI;

(13) Establishes a process to accept and manage challenges to CUI status (which may include improper or absent marking);

(14) Establish processes and criteria for reporting and investigating misuse of CUI; and

(15) Follows the requirements for the CUI SAO listed in §2002.38(e), regarding waivers for CUI.

(d) The Director of National Intelligence: After consulting with the heads of affected agencies and the Director of ISOO, may issue directives to implement this part with respect to the protection of intelligence sources, methods, and activities. Such directives must be in accordance with the Order, this part, and the CUI Registry.

Subpart B—Key Elements of the CUI Program

§2002.10 The CUI Registry.

(a) The CUI EA maintains the CUI Registry, which:

(1) Is the authoritative central repository for all guidance, policy, instructions, and information on CUI (other than the Order and this part);

(2) Is publicly accessible;

(3) Includes authorized CUI categories and subcategories, associated markings, applicable decontrolling procedures, and other guidance and policy information; and

(4) Includes citation(s) to laws, regulations, or Government-wide policies that form the basis for each category and subcategory.

(b) Agencies and authorized holders must follow the instructions contained in the CUI Registry in addition to all requirements in the Order and this part.

§2002.12 CUI categories and subcategories.

(a) CUI categories and subcategories are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies to handle by means of safeguarding or dissemination controls. All unclassified information throughout the executive

branch that requires any kind of safeguarding or dissemination control is CUI. Agencies may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Program.

(b) Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI.

§ 2002.14 Safeguarding.

(a) *General safeguarding policy.* (1) Pursuant to the Order and this part, and in consultation with affected agencies, the CUI EA issues safeguarding standards in this part and, as necessary, in the CUI Registry, updating them as needed. These standards require agencies to safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders.

(2) Safeguarding measures that agencies are authorized or accredited to use for classified information and national security systems are also sufficient for safeguarding CUI in accordance with the organization's management and acceptance of risk.

(3) Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies may not otherwise require controls for CUI Basic at a level higher than permitted in the CUI Basic requirements when disseminating the CUI Basic outside the agency.

(4) Authorized holders must comply with policy in the Order, this part, and the CUI Registry, and review any applicable agency CUI policies for additional instructions. For information designated as CUI Specified, authorized holders must also follow the procedures in the underlying laws, regulations, or Government-wide policies.

(b) *CUI safeguarding standards.* Authorized holders must safeguard CUI using one of the following types of standards:

(1) *CUI Basic.* CUI Basic is the default set of standards authorized holders must apply to all CUI unless the CUI Registry annotates that CUI as CUI Specified.

(2) *CUI Specified.* (i) Authorized holders safeguard CUI Specified in accordance with the requirements of the underlying authorities indicated in the CUI Registry.

(ii) When the laws, regulations, or Government-wide policies governing a specific type of CUI Specified are silent on either a safeguarding or disseminating control, agencies must apply CUI Basic standards to that aspect of the information's controls, unless this results in treatment that does not accord with the CUI Specified authority. In such cases, agencies must apply the CUI Specified standards and may apply limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI Specified authority.

(c) *Protecting CUI under the control of an authorized holder.* Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI. They must include the following measures among the reasonable precautions:

(1) Establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments;

(2) Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI;

(3) Keep CUI under the authorized holder's direct control or protect it with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment; and

(4) Protect the confidentiality of CUI that agencies or authorized holders process, store, or transmit on Federal information systems in accordance with the applicable security requirements and controls established in FIPS PUB 199, FIPS PUB 200, and NIST SP 800–53, (incorporated by reference, see § 2002.2), and paragraph (g) of this section.

(d) *Protecting CUI when shipping or mailing.* When sending CUI, authorized holders:

(1) May use the United States Postal Service or any commercial delivery service when they need to transport or deliver CUI to another entity;

(2) Should use in-transit automated tracking and accountability tools when they send CUI;

(3) May use interoffice or interagency mail systems to transport CUI; and

(4) Must mark packages that contain CUI according to marking requirements contained in this part and in guidance published by the CUI EA. See § 2002.20 for more guidance on marking requirements.

(e) *Reproducing CUI.* Authorized holders:

(1) May reproduce (*e.g.,* copy, scan, print, electronically duplicate) CUI in furtherance of a lawful Government purpose; and

(2) Must ensure, when reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, that the equipment does not retain data or the agency must otherwise sanitize it in accordance with NIST SP 800–53 (incorporated by reference, see § 2002.2).

(f) *Destroying CUI.* (1) Authorized holders may destroy CUI when:

(i) The agency no longer needs the information; and

(ii) Records disposition schedules published or approved by NARA allow.

(2) When destroying CUI, including in electronic form, agencies must do so in a manner that makes it unreadable, indecipherable, and irrecoverable. Agencies must use any destruction method specifically required by law, regulation, or Government-wide policy for that CUI. If the authority does not specify a destruction method, agencies must use one of the following methods:

(i) Guidance for destruction in NIST SP 800–53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800–88, Guidelines for Media Sanitization (incorporated by reference, see § 2002.2); or

(ii) Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or any implementing or successor guidance.

(g) *Information systems that process, store, or transmit CUI.* In accordance with FIPS PUB 199 (incorporated by reference, see § 2002.2), CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines the security impact levels for Federal information and Federal information systems. Agencies must also apply the appropriate security requirements and controls from FIPS PUB 200 and NIST SP 800–53 (incorporated by reference, see § 2002.2) to CUI in accordance with any risk-based tailoring decisions they make. Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside the agency.

(h) Information systems that process, store, or transmit CUI are of two different types:

(1) A Federal information system is an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. An information system operated on behalf of an agency provides information processing services to the agency that the Government might otherwise perform itself but has decided to outsource. This includes systems operated exclusively for Government use and systems operated for multiple users (multiple Federal agencies or Government and private sector users). Information systems that a non-executive branch entity operates on behalf of an agency are subject to the requirements of this part as though they are the agency's systems, and agencies may require these systems to meet additional requirements the agency sets for its own internal systems.

(2) A non-Federal information system is any information system that does not meet the criteria for a Federal information system. Agencies may not treat non-Federal information systems as though they are agency systems, so

agencies cannot require that non-executive branch entities protect these systems in the same manner that the agencies might protect their own information systems. When a non-executive branch entity receives Federal information only incidental to providing a service or product to the Government other than processing services, its information systems are not considered Federal information systems. NIST SP 800–171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

§ 2002.16 Accessing and disseminating.

(a) *General policy*—(1) *Access.* Agencies should disseminate and permit access to CUI, provided such access or dissemination:

(i) Abides by the laws, regulations, or Government-wide policies that established the CUI category or subcategory;

(ii) Furthers a lawful Government purpose;

(iii) Is not restricted by an authorized limited dissemination control established by the CUI EA; and,

(iv) Is not otherwise prohibited by law.

(2) *Dissemination controls.* (i) Agencies must impose dissemination controls judiciously and should do so only to apply necessary restrictions on access to CUI, including those required by law, regulation, or Government-wide policy.

(ii) Agencies may not impose controls that unlawfully or improperly restrict access to CUI.

(3) *Marking.* Prior to disseminating CUI, authorized holders must label CUI according to marking guidance issued by the CUI EA, and must include any specific markings required by law, regulation, or Government-wide policy.

(4) *Reasonable expectation.* To disseminate CUI to a non-executive branch entity, authorized holders must reasonably expect that all intended recipients are authorized to receive the CUI and have a basic understanding of how to handle it.

(5) *Agreements.* Agencies should enter into agreements with any non-executive branch or foreign entity with which the agency shares or intends to share CUI, as follows (except as provided in paragraph (a)(7) of this section):

(i) *Information-sharing agreements.* When agencies intend to share CUI with a non-executive branch entity, they should enter into a formal agreement (see § 2004.4(c) for more information on agreements), whenever feasible. Such an agreement may take any form the agency head approves, but when established, it must include a requirement to comply with Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267) or any successor order (the Order), this part, and the CUI Registry.

(ii) *Sharing CUI without a formal agreement.* When an agency cannot enter into agreements under paragraph (a)(6)(i) of this section, but the agency's mission requires it to disseminate CUI to non-executive branch entities, the agency must communicate to the recipient that the Government strongly encourages the non-executive branch entity to protect CUI in accordance with the Order, this part, and the CUI Registry, and that such protections should accompany the CUI if the entity disseminates it further.

(iii) *Foreign entity sharing.* When entering into agreements or arrangements with a foreign entity, agencies should encourage that entity to protect CUI in accordance with the Order, this part, and the CUI Registry to the extent possible, but agencies may use their judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding

CUI. If such agreements or arrangements include safeguarding or dissemination controls on unclassified information, the agency must not establish a parallel protection regime to the CUI Program: For example, the agency must use CUI markings rather than alternative ones (*e.g.*, such as SBU) for safeguarding or dissemination controls on CUI received from or sent to foreign entities, must abide by any requirements set by the CUI category or subcategory's governing laws, regulations, or Government-wide policies, etc.

(iv) *Pre-existing agreements.* When an agency entered into an information-sharing agreement prior to November 14, 2016, the agency should modify any terms in that agreement that conflict with the requirements in the Order, this part, and the CUI Registry, when feasible.

(6) *Agreement content.* At a minimum, agreements with non-executive branch entities must include provisions that state:

(i) Non-executive branch entities must handle CUI in accordance with the Order, this part, and the CUI Registry;

(ii) Misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies; and

(iii) The non-executive branch entity must report any non-compliance with handling requirements to the disseminating agency using methods approved by that agency's SAO. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency.

(7) *Exceptions to agreements.* Agencies need not enter a written agreement when they share CUI with the following entities:

(i) Congress, including any committee, subcommittee, joint committee, joint subcommittee, or office thereof;

(ii) A court of competent jurisdiction, or any individual or entity when directed by an order of a court of competent jurisdiction or a Federal administrative law judge (ALJ) appointed under 5 U.S.C. 3501;

(iii) The Comptroller General, in the course of performing duties of the Government Accountability Office; or

(iv) Individuals or entities, when the agency releases information to them pursuant to a FOIA or Privacy Act request.

(b) *Controls on accessing and disseminating CUI*—(1) *CUI Basic.* Authorized holders should disseminate and encourage access to CUI Basic for any recipient when the access meets the requirements set out in paragraph (a)(1) of this section.

(2) *CUI Specified.* Authorized holders disseminate and allow access to CUI Specified as required or permitted by the authorizing laws, regulations, or Government-wide policies that established that CUI Specified.

(i) The CUI Registry annotates CUI that requires or permits Specified controls based on law, regulation, and Government-wide policy.

(ii) In the absence of specific dissemination restrictions in the authorizing law, regulation, or Government-wide policy, agencies may disseminate CUI Specified as they would CUI Basic.

(3) *Receipt of CUI.* Non-executive branch entities may receive CUI directly from members of the executive branch or as sub-recipients from other non-executive branch entities.

(4) *Limited dissemination.* (i) Agencies may place additional limits on disseminating CUI only through use of the limited dissemination controls approved by the CUI EA and published in the CUI Registry. These limited dissemination controls are separate from any controls that a CUI Specified authority requires or permits.

(ii) Using limited dissemination controls to unnecessarily restrict access to CUI is contrary to the goals of the CUI Program. Agencies may therefore use these controls only when it furthers a lawful Government purpose, or laws, regulations, or Government-wide policies require or permit an agency to do so. If an authorized holder has significant doubt about whether it is appropriate to use a limited dissemination control, the authorized holder should consult with and follow the designating agency's policy. If, after consulting the policy, significant doubt still remains,

the authorized holder should not apply the limited dissemination control.

(iii) Only the designating agency may apply limited dissemination controls to CUI. Other entities that receive CUI and seek to apply additional controls must request permission to do so from the designating agency.

(iv) Authorized holders may apply limited dissemination controls to any CUI for which they are required or permitted to restrict access by or to certain entities.

(v) Designating entities may combine approved limited dissemination controls listed in the CUI Registry to accommodate necessary practices.

(c) *Methods of disseminating CUI.* (1) Before disseminating CUI, authorized holders must reasonably expect that all intended recipients have a lawful Government purpose to receive the CUI. Authorized holders may then disseminate the CUI by any method that meets the safeguarding requirements of this part and the CUI Registry and ensures receipt in a timely manner, unless the laws, regulations, or Government-wide policies that govern that CUI require otherwise.

(2) To disseminate CUI using systems or components that are subject to NIST guidelines and publications (*e.g.*, email applications, text messaging, facsimile, or voicemail), agencies must do so in accordance with the no-less-than-moderate confidentiality impact value set out in FIPS PUB 199, FIPS PUB 200, NIST SP 800–53 (incorporated by reference, see § 2002.2).

§ 2002.18 Decontrolling.

(a) Agencies should decontrol as soon as practicable any CUI designated by their agency that no longer requires safeguarding or dissemination controls, unless doing so conflicts with the governing law, regulation, or Government-wide policy.

(b) Agencies may decontrol CUI automatically upon the occurrence of one of the conditions below, or through an affirmative decision by the designating agency:

(1) When laws, regulations or Government-wide policies no longer require its control as CUI and the authorized holder has the appropriate authority under the authorizing law, regulation, or Government-wide policy;

(2) When the designating agency decides to release it to the public by making an affirmative, proactive disclosure;

(3) When the agency discloses it in accordance with an applicable information access statute, such as the FOIA, or the Privacy Act (when legally permissible), if the agency incorporates such disclosures into its public release processes; or

(4) When a pre-determined event or date occurs, as described in § 2002.20(g), unless law, regulation, or Government-wide policy requires coordination first.

(c) The designating agency may also decontrol CUI:

(1) In response to a request by an authorized holder to decontrol it; or

(2) Concurrently with any declassification action under Executive Order 13526 or any predecessor or successor order, as long as the information also appropriately qualifies for decontrol as CUI.

(d) An agency may designate in its CUI policies which agency personnel it authorizes to decontrol CUI, consistent with law, regulation, and Government-wide policy.

(e) Decontrolling CUI relieves authorized holders from requirements to handle the information under the CUI Program, but does not constitute authorization for public release.

(f) Authorized holders must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, releasing to the public, or donating it to a private institution. Otherwise, authorized holders do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

(1) Agency policy may allow authorized holders to remove or strike through only those CUI markings on the first or cover page of the decontrolled CUI and markings on the first page of any attachments that contain CUI.

(2) If an authorized holder uses the decontrolled CUI in a newly created document, the authorized holder must remove all CUI markings for the decontrolled information.

(g) Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and agency policies on the public release of information.

(h) Authorized holders may request that the designating agency decontrol certain CUI.

(i) If an authorized holder publicly releases CUI in accordance with the designating agency's authorized procedures, the release constitutes decontrol of the information.

(j) Unauthorized disclosure of CUI does not constitute decontrol.

(k) Agencies must not decontrol CUI in an attempt to conceal, or to otherwise circumvent accountability for, an identified unauthorized disclosure.

(l) When laws, regulations, or Government-wide policies require specific decontrol procedures, authorized holders must follow such requirements.

(m) The Archivist of the United States may decontrol records transferred to the National Archives in accordance with § 2002.34, absent a specific agreement otherwise with the designating agency. The Archivist decontrols records to facilitate public access pursuant to 44 U.S.C. 2108 and NARA's regulations at 36 CFR parts 1235, 1250, and 1256.

§ 2002.20 Marking.

(a) *General marking policy.* (1) CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls. Agencies and authorized holders must, in accordance with the implementation timelines established for the agency by the CUI EA:

(i) Discontinue all use of legacy or other markings not permitted by this part or included in the CUI Registry; and

(ii) Uniformly and conspicuously apply CUI markings to all CUI exclusively in accordance with the part and the CUI Registry, unless this part or the CUI EA otherwise specifically permits. See paragraph (a)(6) of this section and §§ 2002.38, Waivers of CUI requirements, and 2002.36, Legacy materials, for more information.

(2) Agencies may not modify CUI Program markings or deviate from the method of use prescribed by the CUI EA (in this part and the CUI Registry) in an effort to accommodate existing agency marking practices, except in circumstances approved by the CUI EA. The CUI Program prohibits using markings or practices not included in this part or the CUI Registry. If legacy markings remain on information, the legacy markings are void and no longer indicate that the information is protected or that it is or qualifies as CUI.

(3) An agency receiving an incorrectly marked document should notify either the disseminating entity or the designating agency, and request a properly marked document.

(4) The designating agency determines that the information qualifies for CUI status and applies the appropriate CUI marking when it designates that information as CUI.

(5) If an agency has information within its control that qualifies as CUI but has not been previously marked as CUI for any reason (for example, pursuant to an agency internal marking waiver as referenced in § 2002.38 (a)), the agency must mark it as CUI prior to disseminating it.

(6) Agencies must not mark information as CUI to conceal illegality, negligence, ineptitude, or other disreputable circumstances embarrassing to any person, any agency, the Federal Government, or any of their partners, or for any purpose other than to adhere to the law, regulation, or Government-wide policy authorizing the control.

(7) The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable handling requirements as described in the Order, this part, and the CUI Registry.

(8) When it is impractical for an agency to individually mark CUI due to quantity or nature of the information, or when an agency has issued a limited CUI marking waiver, authorized holders must make recipients aware of the information's CUI status using an alternate marking method that is readily apparent (for example, through user access agreements, a computer system digital splash screen (*e.g.*, alerts that flash up when accessing the system), or signs in storage areas or on containers).

(b) *The CUI banner marking.* Designators of CUI must mark all CUI with a CUI banner marking, which may include up to three elements:

(1) *The CUI control marking (mandatory).* (i) The CUI control marking may consist of either the word ''CONTROLLED'' or the acronym ''CUI,'' at the designator's discretion. Agencies may specify in their CUI policy that employees must use one or the other.

(ii) The CUI Registry contains additional, specific guidance and instructions for using the CUI control marking.

(iii) Authorized holders who designate CUI may not use alternative markings to identify or mark items as CUI.

(2) *CUI category or subcategory markings (mandatory for CUI Specified).* (i) The CUI Registry lists the category and subcategory markings, which align with the CUI's governing category or subcategory.

(ii) Although the CUI Program does not require agencies to use category or subcategory markings on CUI Basic, an agency's CUI SAO may establish agency policy that mandates use of CUI category or subcategory markings on CUI Basic.

(iii) However, authorized holders must include in the CUI banner marking all CUI Specified category or subcategory markings that pertain to the information in the document. If law, regulation, or Government-wide policy requires specific marking, disseminating, informing, distribution limitation, or warning statements, agencies must use those indicators as those authorities require or permit. However, agencies must not include these additional indicators in the CUI banner marking or CUI portion markings.

(iv) The CUI Registry contains additional, specific guidance and instructions for using CUI category and subcategory markings.

(3) *Limited dissemination control markings.* (i) CUI limited dissemination control markings align with limited dissemination controls established by the CUI EA under § 2002.16(b)(4).

(ii) Agency policy should include specific criteria establishing which authorized holders may apply limited dissemination controls and their corresponding markings, and when. Such agency policy must align with the requirements in § 2002.16(b)(4).

(iii) The CUI Registry contains additional, specific guidance and instructions for using limited dissemination control markings.

(c) *Using the CUI banner marking.* (1) The content of the CUI banner marking must apply to the whole document (*i.e.*, inclusive of all CUI within the document) and must be the same on each page of the document that includes CUI.

(2) The CUI Registry contains additional, specific guidelines and instructions for using the CUI banner marking.

(d) *CUI designation indicator (mandatory).* (1) All documents containing CUI must carry an indicator of who designated the CUI within it. This must include the designator's agency (at a minimum) and may take any form that identifies the designating agency, including letterhead or other standard agency indicators, or adding a ''Controlled by'' line (for example, ''Controlled by: Division 5, Department of Good Works.'').

(2) The designation indicator must be readily apparent to authorized holders and may appear only on the first page or cover. The CUI Registry contains additional, specific guidance and requirements for using CUI designation indicators.

(e) *CUI decontrolling indicators.* (1) Where feasible, designating agencies must include a specific decontrolling date or event with all CUI. Agencies may do so in any manner that makes the decontrolling schedule readily apparent to an authorized holder.

(2) Authorized holders may consider specific items of CUI as decontrolled as of the date indicated, requiring no further review by, or communication with, the designator.

(3) If using a specific event after which the CUI is considered decontrolled:

(i) The event must be foreseeable and verifiable by any authorized holder (*e.g.*, not based on or requiring special access or knowledge); and

(ii) The designator should include point of contact and preferred method of contact information in the decontrol

indicator when using this method, to allow authorized holders to verify that a specified event has occurred.

(4) The CUI Registry contains additional, specific guidance and instructions for using limited dissemination control markings.

(f) *Portion marking CUI.* (1) Agencies are permitted and encouraged to portion mark all CUI, to facilitate information sharing and proper handling.

(2) Authorized holders who designate CUI may mark CUI only with portion markings approved by the CUI EA and listed in the CUI Registry.

(3) CUI portion markings consist of the following elements:

(i) The CUI control marking, which must be the acronym ''CUI'';

(ii) CUI category/subcategory portion markings (if required or permitted); and

(iii) CUI limited dissemination control portion markings (if required).

(4) When using portion markings:

(i) CUI category and subcategory portion markings are optional for CUI Basic. Agencies may manage their use by means of agency policy.

(ii) Authorized holders permitted to designate CUI must portion mark both CUI and uncontrolled unclassified portions.

(5) In cases where portions consist of several segments, such as paragraphs, sub-paragraphs, bullets, and sub-bullets, and the control level is the same throughout, designators of CUI may place a single portion marking at the beginning of the primary paragraph or bullet. However, if the portion includes different CUI categories or subcategories, or if the portion includes some CUI and some uncontrolled unclassified information, authorized holders should portion mark all segments separately to avoid improper control of any one segment.

(6) Each portion must reflect the control level of only that individual portion. If the information contained in a sub-paragraph or sub-bullet is a different CUI category or subcategory from its parent paragraph or parent bullet, this does not make the parent paragraph or parent bullet controlled at that same level.

(7) The CUI Registry contains additional, specific guidance and instructions for using CUI portion markings and uncontrolled unclassified portion markings.

(g) *Commingling CUI markings with Classified National Security Information (CNSI).* When authorized holders include CUI in documents that also contain CNSI, the decontrolling provisions of the Order and this part apply only to portions marked as CUI. In addition, authorized holders must:

(1) Portion mark all CUI to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information;

(2) Include the CUI control marking, CUI Specified category and subcategory markings, and limited dissemination control markings in an overall banner marking; and

(3) Follow the requirements of the Order and this part, and instructions in the CUI Registry on marking CUI when commingled with CNSI.

(h) *Commingling restricted data (RD) and formerly restricted data (FRD) with CUI.* (1) To the extent possible, avoid commingling RD or FRD with CUI in the same document. When it is not practicable to avoid such commingling, follow the marking requirements in the Order and this part, and instructions in the CUI Registry, as well as the marking requirements in 10 CFR part 1045, Nuclear Classification and Declassification.

(2) Follow the requirements of 10 CFR part 1045 when extracting an RD or FRD portion for use in a new document.

(3) Follow the requirements of the Order and this part, and instructions in the CUI Registry if extracting a CUI portion for use in a new document.

(4) The lack of declassification instructions for RD or FRD portions does not eliminate the requirement to process commingled documents for declassification in accordance with the Atomic Energy Act, or 10 CFR part 1045.

(i) *Packages and parcels containing CUI.* (1) Address packages that contain CUI for delivery only to a specific recipient.

(2) Do not put CUI markings on the outside of an envelope or package, or

otherwise indicate on the outside that the item contains CUI.

(j) *Transmittal document marking requirements.* (1) When a transmittal document accompanies CUI, the transmittal document must include a CUI marking on its face (''CONTROLLED'' or ''CUI''), indicating that CUI is attached or enclosed.

(2) The transmittal document must also include conspicuously on its face the following or similar instructions, as appropriate:

(i) ''When enclosure is removed, this document is Uncontrolled Unclassified Information''; or

(ii) ''When enclosure is removed, this document is (control level); upon removal, this document does not contain CUI.''

(k) *Working papers.* Mark working papers containing CUI the same way as the finished product containing CUI would be marked and as required for any CUI contained within them. Handle them in accordance with this part and the CUI Registry.

(l) *Using supplemental administrative markings with CUI.* (1) Agency heads may authorize the use of supplemental administrative markings (*e.g.* ''Predecisional,'' ''Deliberative,'' ''Draft'') for use with CUI.

(2) Agency heads may not authorize the use of supplemental administrative markings to establish safeguarding requirements or disseminating restrictions, or to designate the information as CUI. However, agencies may use these markings to inform recipients of the non-final status of documents under development to avoid confusion and maintain the integrity of an agency's decision-making process.

(3) Agencies must detail requirements for using supplemental administrative markings with CUI in agency policy that is available to anyone who may come into possession of CUI with these markings.

(4) Authorized holders must not incorporate or include supplemental administrative markings in the CUI marking scheme detailed in this part and the CUI Registry.

(5) Supplemental administrative markings must not duplicate any CUI marking described in this part or the CUI Registry.

(m) *Unmarked CUI.* Treat unmarked information that qualifies as CUI as described in the Order, § 2002.8(c), and the CUI Registry.

§ 2002.22 Limitations on applicability of agency CUI policies.

(a) Agency CUI policies do not apply to entities outside that agency unless a law, regulation, or Government-wide policy requires or permits the controls contained in the agency policy to do so, and the CUI Registry lists that law, regulation, or Government-wide policy as a CUI authority.

(b) Agencies may not include additional requirements or restrictions on handling CUI other than those permitted in the Order, this part, or the CUI Registry when entering into agreements.

§ 2002.24 Agency self-inspection program.

(a) The agency must establish a self-inspection program pursuant to the requirement in § 2002.8(b)(4).

(b) The self-inspection program must include:

(1) At least annual review and assessment of the agency's CUI program. The agency head or CUI SAO should determine any greater frequency based on program needs and the degree to which the agency engages in designating CUI;

(2) Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;

(3) Formats for documenting self-inspections and recording findings when not prescribed by the CUI EA;

(4) Procedures by which to integrate lessons learned and best practices arising from reviews and assessments into operational policies, procedures, and training;

(5) A process for resolving deficiencies and taking corrective actions; and

(6) Analysis and conclusions from the self-inspection program, documented on an annual basis and as requested by the CUI EA.

Subpart C—CUI Program Management

§ 2002.30 Education and training.

(a) The CUI SAO must establish and implement an agency training policy. At a minimum, the training policy must address the means, methods, and frequency of agency CUI training.

(b) Agency training policy must ensure that personnel who have access to CUI receive training on designating CUI, relevant CUI categories and subcategories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures.

(c) Agencies must train employees on these matters when the employees first begin working for the agency and at least once every two years thereafter.

(d) The CUI EA reviews agency training materials to ensure consistency and compliance with the Order, this part, and the CUI Registry.

§ 2002.32 CUI cover sheets.

(a) Agencies may use cover sheets for CUI. If an agency chooses to use cover sheets, it must use CUI EA-approved cover sheets, which agencies can find on the CUI Registry.

(b) Agencies may use cover sheets to identify CUI, alert observers that CUI is present from a distance, and serve as a shield to protect the attached CUI from inadvertent disclosure.

§ 2002.34 Transferring records.

(a) When feasible, agencies must decontrol records containing CUI prior to transferring them to NARA.

(b) When an agency cannot decontrol records before transferring them to NARA, the agency must:

(1) Indicate on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI (subject to NARA's regulations on transfer, public availability, and access; see 36 CFR parts 1235, 1250, and 1256); and

(2) For hard copy transfer, do not place a CUI marking on the outside of the container.

(c) If the agency does not indicate the status as CUI on the TR or SF 258, NARA may assume the agency decontrolled the information prior to transfer, regardless of any CUI markings on the actual records.

§ 2002.36 Legacy materials.

(a) Agencies must review documents created prior to November 14, 2016 and re-mark any that contain information that qualifies as CUI in accordance with the Order, this part, and the CUI Registry. When agencies do not individually re-mark legacy material that qualifies as CUI, agencies must use an alternate permitted marking method (see § 2002.20(a)(8)).

(b) When the CUI SAO deems remarking legacy documents to be excessively burdensome, the CUI SAO may grant a legacy material marking waiver under § 2002.38(b).

(c) When the agency re-uses any information from legacy documents that qualifies as CUI, whether the documents have obsolete control markings or not, the agency must designate the newly-created document (or other reuse) as CUI and mark it accordingly.

§ 2002.38 Waivers of CUI requirements.

(a) *Limited CUI marking waivers within the agency.* When an agency designates information as CUI but determines that marking it as CUI is excessively burdensome, an agency's CUI SAO may approve waivers of all or some of the CUI marking requirements while that CUI remains within agency control.

(b) *Limited legacy material marking waivers within the agency.* (1) In situations in which the agency has a substantial amount of stored information with legacy markings, and removing legacy markings and designating or remarking it as CUI would be excessively burdensome, the agency's CUI SAO may approve a waiver of these requirements for some or all of that information while it remains under agency control.

(2) When an authorized holder re-uses any legacy information or information derived from legacy documents that qualifies as CUI, they must remove or redact legacy markings and designate or re-mark the information as CUI, even if the information is under a legacy material marking waiver prior to re-use.

(c) *Exigent circumstances waivers.* (1) In exigent circumstances, the agency head or the CUI SAO may waive the provisions and requirements established in this part or the CUI Registry for any CUI while it is within the agency's possession or control, unless specifically prohibited by applicable laws, regulations, or Government-wide policies.

(2) Exigent circumstances waivers may apply when an agency shares the information with other agencies or non-Federal entities. In such cases, the authorized holders must make recipients aware of the CUI status of any disseminated information.

(d) *For all waivers.* (1) The CUI SAO must still ensure that the agency appropriately safeguards and disseminates the CUI. See § 2002.20(a)(7);

(2) The CUI SAO must detail in each waiver the alternate protection methods the agency will employ to ensure protection of CUI subject to the waiver;

(3) All marking waivers apply to CUI subject to the waiver only while that agency continues to possess that CUI. No marking waiver may accompany CUI when an authorized holder disseminates it outside that agency;

(4) Authorized holders must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it outside the agency unless otherwise specifically permitted by the CUI EA; and

(5) When the circumstances requiring the waiver end, the CUI SAO must reinstitute the requirements for all CUI subject to the waiver without delay.

(e) The CUI SAO must:

(1) Retain a record of each waiver;

(2) Include a description of all current waivers and waivers issued during the preceding year in the annual report to the CUI EA, along with the rationale for each waiver and the alternate steps the agency takes to ensure sufficient protection of CUI; and

(3) Notify authorized recipients and the public of these waivers.

§ 2002.44 CUI and disclosure statutes.

(a) *General policy.* The fact that an agency designates certain information as CUI does not affect an agency's or employee's determinations pursuant to any law that requires the agency or the employee to disclose that information or permits them to do so as a matter of discretion. The agency or employee must make such determinations according to the criteria set out in the governing law, not on the basis of the information's status as CUI.

(b) *CUI and the Freedom of Information Act (FOIA).* Agencies must not cite the FOIA as a CUI safeguarding or disseminating control authority for CUI. When an agency is determining whether to disclose information in response to a FOIA request, the agency must base its decision on the content of the information and applicability of any FOIA statutory exemptions, regardless of whether an agency designates or marks the information as CUI. There may be circumstances in which an agency may disclose CUI to an individual or entity, including through a FOIA response, but such disclosure does not always constitute public release as defined in this part. Although disclosed via a FOIA response, the agency may still need to control the CUI while the agency continues to hold the information, despite the disclosure, unless the agency otherwise decontrols it (or the agency includes in its policies that FOIA disclosure always results in public release and the CUI does not otherwise have another legal requirement for its continued control).

(c) *CUI and the Whistleblower Protection Act.* This part does not change or affect existing legal protections for whistleblowers. The fact that an agency designates or marks certain information as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority, and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, or executive order or directive.

§ 2002.46 CUI and the Privacy Act.

The fact that records are subject to the Privacy Act of 1974 does not mean that agencies must mark them as CUI. Consult agency policies or guidance to determine which records may be subject to the Privacy Act; consult the CUI Registry to determine which privacy information must be marked as CUI. Information contained in Privacy

Act systems of records may also be subject to controls under other CUI categories or subcategories and the agency may need to mark that information as CUI for that reason. In addition, when determining whether the agency must protect certain information under the Privacy Act, or whether the Privacy Act allows the agency to release the information to an individual, the agency must base its decision on the content of the information and the Privacy Act's criteria, regardless of whether an agency designates or marks the information as CUI.

§ 2002.48 CUI and the Administrative Procedure Act (APA).

Nothing in the regulations in this part alters the Administrative Procedure Act (APA) or the powers of Federal administrative law judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor do the regulations in this part impose requirements concerning the manner in which ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

§ 2002.50 Challenges to designation of information as CUI.

(a) Authorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the disseminating agency of this belief. When the disseminating agency is not the designating agency, the disseminating agency must notify the designating agency.

(b) If the information at issue is involved in Government litigation, or the challenge to its designation or marking as CUI arises as part of the litigation, the issue of whether the challenger may access the information will be addressed via the litigation process instead of by the agency CUI program. Challengers should nonetheless notify the agency of the issue through the agency process described below, and include its litigation connection.

(c) CUI SAOs must create a process within their agency to accept and manage challenges to CUI status. At a minimum, this process must include a timely response to the challenger that:

(1) Acknowledges receipt of the challenge;

(2) States an expected timetable for response to the challenger;

(3) Provides an opportunity for the challenger to define a rationale for belief that the CUI in question is inappropriately designated;

(4) Gives contact information for the official making the agency's decision in this matter; and

(5) Ensures that challengers who are authorized holders have the option of bringing such challenges anonymously, and that challengers are not subject to retribution for bringing such challenges.

(d) Until the challenge is resolved, authorized holders should continue to safeguard and disseminate the challenged CUI at the control level indicated in the markings.

(e) If a challenging party disagrees with the response to a challenge, that party may use the Dispute Resolution procedures described in § 2002.52.

§ 2002.52 Dispute resolution for agencies.

(a) When laws, regulations, or Government-wide policies governing the CUI involved in a dispute set out specific procedures, processes, and requirements for resolving disputes, agencies must follow those processes for that CUI. This includes submitting the dispute to someone other than the CUI EA for resolution if the authority so requires. If the CUI at issue is involved in litigation, the agency should refer the issue to the appropriate attorneys for resolution through the litigation process.

(b) When laws, regulations, and Government-wide policies governing the CUI do not set out specific procedures, processes, or requirements for CUI dispute resolution (or the information is not involved in litigation), this part governs.

(c) All parties to a dispute arising from implementing or interpreting the Order, this part, or the CUI Registry should make every effort to resolve the dispute expeditiously. Parties should address disputes within a reasonable,

mutually acceptable time period, taking into consideration the parties' mission, sharing, and protection requirements.

(d) If parties to a dispute cannot reach a mutually acceptable resolution, either party may refer the matter to the CUI EA.

(e) The CUI EA acts as the impartial arbiter of the dispute and has the authority to render a decision on the dispute after consulting with all affected parties. If a party to the dispute is also a member of the Intelligence Community, the CUI EA must consult with the Office of the Director of National Intelligence when the CUI EA receives the dispute for resolution.

(f) Until the dispute is resolved, authorized holders should continue to safeguard and disseminate any disputed CUI at the control level indicated in the markings, or as directed by the CUI EA if the information is unmarked.

(g) Parties may appeal the CUI EA's decision through the Director of OMB to the President for resolution, pursuant to section 4(e) of the Order. If one of the parties to the dispute is the CUI EA and the parties cannot resolve the dispute under paragraph (c) of this section, the parties may likewise refer the matter to OMB for resolution.

§ 2002.54 Misuse of CUI.

(a) The CUI SAO must establish agency processes and criteria for reporting and investigating misuse of CUI.

(b) The CUI EA reports findings on any incident involving misuse of CUI to the offending agency's CUI SAO or CUI Program manager for action, as appropriate.

§ 2002.56 Sanctions for misuse of CUI.

(a) To the extent that agency heads are otherwise authorized to take administrative action against agency personnel who misuse CUI, agency CUI policy governing misuse should reflect that authority.

(b) Where laws, regulations, or Government-wide policies governing certain categories or subcategories of CUI specifically establish sanctions, agencies must adhere to such sanctions.

APPENDIX A TO PART 2002—ACRONYMS

CNSI—Classified National Security Information
Council or the Council—The CUI Advisory Council
CUI—Controlled unclassified information
EA—The CUI Executive Agent (which is ISOO)
FOIA—Freedom of Information Act
FRD—Formerly Restricted Data
ISOO—Information Security Oversight Office at the National Archives and Records Administration
NARA—National Archives and Records Administration
OMB—Office of Management and Budget within the Office of Information and Regulatory Affairs of the Executive Office of the President
PM—the agency's CUI program manager
RD—Restricted Data
SAO—the senior agency official [for CUI]
TR—Transfer Request in NARA's Electronic Records Archives (ERA)

PART 2003—INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL (ISCAP) BYLAWS, RULES, AND APPEAL PROCEDURES

Subpart A—Bylaws

Sec.

Subpart B—Appeal Procedures

AUTHORITY: E.O. 13526, 75 FR 707, 75 FR 1013, 3 CFR, 2010 Comp., p. 298

SOURCE: 77 FR 40261, July 9, 2012, unless otherwise noted.

Subpart A—Bylaws

§ 2003.1 Purpose (Article I).

The Interagency Security Classification Appeals Panel (hereafter ''ISCAP'' or ''the Panel'') advises and assists the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States.

§ 2003.2 Authority (Article II).

ISCAP was established by, and receives its authority from, Executive Order 13526 ''Classified National Security Information'' (hereafter the ''Order''), December 29, 2009, section 5.3(a)(1), and the Order's implementing directives. Section 5.3(c) of the Order directs ISCAP to issue bylaws, rules, and procedures and to publish them in the FEDERAL REGISTER.

§ 2003.3 Functions (Article III).

In carrying out its purpose, the Panel:

(a) Decides appeals by people who have filed classification challenges under section 1.8 of the Order;

(b) Approves, denies, or amends agency exemptions from automatic declassification under section 3.3 of the Order;

(c) Decides appeals by people or entities who have filed requests for mandatory declassification review under section 3.5 of the Order; and

(d) Informs senior agency officials and the public, as appropriate, of final Panel decisions on appeals under sections 1.8 and 3.5 of the Order.

§ 2003.4 Membership (Article IV).

(a) *Member organizations and members.* (1) The Departments of State, Defense, and Justice, the National Archives and Records Administration, the Office of the Director of National Intelligence, and the National Security Advisor each have a member on the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative, who meets the member criteria, to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(b) *Alternate member.* Each member organization also designates in writing an alternate, or alternates, to represent it on all occasions when the primary member is unable to participate. When serving for a primary member, an alternate assumes all the rights and responsibilities of that primary member, including voting. The alternate member must meet the member criteria. The member organization head, or the organization's deputy or senior agency official for the Order, makes the written designation of an alternate, addressed to the ISCAP Chair.

(c) *Selection criteria for member.* (1) Members must be senior-level agency Federal officials or employees, full-time or permanent part-time, and must be designated to serve as a member on the Panel by the respective agency head.

(2) Panel members must meet security access criteria in order to fulfill the Panel's functions.

(d) *Member vacancies.* Vacancies among the primary members must be filled as quickly as possible. The Chair, working through the Executive Secretary, takes all appropriate measures to encourage the organization to fill the vacancy quickly. In the interim, the organization's designated alternate serves as its member.

(e) *Liaisons.* Each member organization also designates in writing an individual or individuals (hereafter ''liaisons'') to serve as liaison to the Executive Secretary in support of the primary member and alternate(s). The liaisons meet at the call of the Executive Secretary. The agency head, or the deputy or senior agency official for the Order, makes the written designation, addressed to the ISCAP Chair.

(f) *Chair.* The President of the United States selects the Chair from among the primary members.

(g) *Vice Chair.* The members may elect from among the primary members a Vice Chair who:

(1) Chairs meetings that the Chair is unable to attend; and

(2) Serves as Acting Chair during a vacancy in the Chair of the ISCAP.

(h) *Executive Secretary*. The Director of the Information Security Oversight Office (ISOO), National Archives and Records Administration, is the Executive Secretary of the Panel and oversees the Panel's support staff.

§ 2003.5 Meetings (Article V).

(a) *Purpose*. The primary purpose of ISCAP meetings is to discuss and bring formal resolution to matters before the Panel and carry out the functions listed in § 2003.3, Article III, of these bylaws.

(b) *Frequency*. The Panel meets at the call of the Chair, who schedules meetings as necessary for the Panel to fulfill its functions in a timely manner. The Chair also convenes the ISCAP when requested by a majority of its member organizations.

(c) *Quorum*. Panel meetings may be held only when a quorum is present. For this purpose, a quorum requires the presence of at least five primary or alternate members.

(d) *Attendance*. As determined by the Chair, attendance at Panel meetings is limited to only the people necessary for the Panel to fulfill its functions in a complete and timely manner. The members may arrange briefings by substantive experts from individual departments or agencies, after consultation with the Chair.

(e) *Agenda*. The Chair establishes the agenda for all meetings. Any member or the Executive Secretary may submit potential items for the agenda. Acting through the Executive Secretary, the Chair distributes the agenda and supporting materials to the members as soon as possible before a scheduled meeting.

(f) *Minutes*. The Executive Secretary and staff prepare each meeting's minutes, and distribute draft minutes to each member. The minutes include a record of the members present at the meeting and the result of each vote. At each Panel meeting, the Chair reads or references the previous meeting's draft minutes. At that time the minutes are corrected, as necessary, approved by the membership, and certified by the Chair. The approved minutes are maintained among the Panel's records.

§ 2003.6 Voting (Article VI).

(a) *Motions*. When the Panel is required to make a decision or recommendation to resolve a matter before it, the Chair requests or accepts a motion for a vote. Any member, including the Chair, may make a motion for a vote. No second is required to bring any motion to a vote. A quorum must be present when a vote is taken.

(b) *Eligibility*. Only the member, including the Chair, may vote on a motion before the ISCAP, with each represented member organization having one vote.

(c) *Voting procedures at meetings*. Votes are ordinarily 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. A motion passes when it receives a majority of affirmative votes of the members voting. In circumstances in which members abstain from voting, a Panel decision to reverse an agency's classification decision requires the affirmative vote of at least a majority of the members present.

(e) *Votes in a non-meeting context*. 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 be present. The Executive Secretary records and retains such votes in a documentary form and immediately reports the results to the Chair and other primary or alternate members, including all notes of concurrence or dissent. If a member expresses dissent to taking a non-meeting vote, any member may request the Chair call a meeting of the members to discuss the issue under consideration and to hold an in-person vote.

§ 2003.7 Support Staff (Article VII).

The staff of the Information Security Oversight Office (ISOO), National Archives and Records Administration, provides program and administrative support for the Panel. The Executive Secretary supervises the staff in this function pursuant to the direction of the Chair and ISCAP. On an as-needed basis, the Panel may seek detailees from agencies to augment the ISOO staff in support of the ISCAP. All staff

must meet security access criteria in order to fulfill the Panel's functions.

§ 2003.8 Records (Article VIII).

(a) *Integrity of ISCAP Records*. The Executive Secretary maintains records that are produced by or presented to the ISCAP or its staff in the performance of the Panel's functions, consistent with applicable law.

(b) *Access requests or Freedom of Information Act (FOIA) requests for ISCAP records*. The Panel refers any FOIA request or other access request for information that originated within an agency other than the ISCAP to that agency for processing. The Panel processes requests for information originated by the ISCAP in accordance with 44 U.S.C. sections 2201–2207 (Presidential Records Act).

(c) *Disposition*. The Executive Secretary maintains Panel records in accordance with 44 U.S.C. sections 2201–2207 (Presidential Records Act).

§ 2003.9 Reports to the President (Article IX).

ISOO includes pertinent information and data about the activities of the Panel in ISOO's reports to the President of the United States. The Panel also includes such information in any reports it may make to the President. The Chair, in coordination with the other members of the ISCAP and the Executive Secretary, determines what information and data to include in each report.

§ 2003.10 Approval, amendment, and publication of bylaws, rules, and procedures (Article X).

Approval and amendment of Panel bylaws, rules, and procedures requires the affirmative vote of at least four members. The Executive Secretary submits approved bylaws, rules, procedures, and their amendments, for publication in the FEDERAL REGISTER.

Subpart B—Appeal Procedures

§ 2003.11 Appeals of agency decisions regarding classification challenges under section 1.8 of the Order.

Authorized holders of information who, in good faith, believe that its classification status is improper may challenge an agency's classification of the information in accordance with agency procedures. After challenging the classification at the agency level, the authorized holder may appeal the agency's decision to the ISCAP.

(a) *Jurisdiction*. The ISCAP will consider and decide appeals from classification challenges that otherwise meet the standards of the Order if:

(1) The appeal is filed in accordance with these procedures;

(2) The appellant has previously challenged the classification action at the agency that originated, or is otherwise responsible for, the information in question. The previous challenge must have followed the agency's established procedures or, if the agency has failed to establish procedures, the appellant must have filed a written challenge directly with the agency head or designated senior agency official, as defined in section 5.4(d) of the Order;

(3) The appellant has:

(i) Received a final agency decision denying his or her challenge; or

(ii) Not received—

(A) An initial written response to the classification challenge from the agency within 120 days of its filing, or

(B) A written response to an agency level 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;

(5) The information in question has not been the subject of a FOIA or mandatory declassification review within the past two years; and

(6) The information in question has not been the subject of a prepublication review or other administrative process pursuant to an approved nondisclosure agreement.

(b) *Submission of appeals*. Appeals may be submitted to the Panel by email or mail. Appeals should be sent via email to: *ISCAP@nara.gov* or by mail to: Executive Secretary, Interagency Security Classification Appeals Panel; Attn: Classification Challenge Appeals; c/o Information Security Oversight Office; National Archives and Records Administration; 700 Pennsylvania Avenue NW., Room 503; Washington, DC 20408.

(1) 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.

(2) No classified information should be included within the initial appeal correspondence. 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 Panel in one of the two methods listed above.

(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)(i) and (ii) of this section.

(d) *Rejection of appeals.* If the Executive Secretary determines that an appeal does not meet the requirements of the Order or these bylaws, the Executive Secretary notifies the appellant in writing that the appeal will not be considered by the ISCAP. The notification includes an explanation of why the appeal is deficient.

(e) *Preparation of appeals and creation of appeals files.* The Executive Secretary notifies the designated senior agency official, and, if applicable, the primary member, alternate, or liaison of the affected agency(ies) when an appeal is lodged. Under the direction of the ISCAP, the Executive Secretary supervises the preparation of an appeal file, pertinent portions of which are presented to the members of the Panel for review prior to a vote on the appeal. The appeal file eventually includes all records pertaining to the appeal.

(f) *Resolution of appeals.* The Panel 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. In circumstances in which members abstain from voting, a Panel decision to reverse an agency's classification decision requires the affirmative vote of at least a majority of the members present.

(g) *Notification.* The Executive Secretary promptly notifies the appellant and the designated senior agency official in writing of the Panel'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 National Security Advisor to overrule the Panel's decision. The information at issue remains classified until the President has issued a decision.

(i) *Protection of classified information.* All persons involved in the appeal will make every effort to minimize the inclusion of classified information in the appeal file. Any classified information contained in the appeal file is handled and protected in accordance with the Order and its implementing directives. Information being challenged for classification remains classified unless and until a final decision is made to declassify it.

(j) *Maintenance and disposition of file.* The Executive Secretary maintains the appeal file among the ISCAP's records in accordance with 44 U.S.C. 2201–2207 (the Presidential Records Act).

§ 2003.12 Review of agency exemptions from automatic declassification under section 3.3 of the Order.

All classified records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code, are automatically declassified whether or not the records have been reviewed. However, agency heads may exempt information that would otherwise fall into this category on specific bases set out in section 3.3 of the Order. The ISCAP reviews and approves, denies, or amends agency proposals to exempt such information from automatic declassification.

(a) *Agency notification of exemptions.* The agency head or designated senior agency official notifies the Executive Secretary of proposed agency exemptions in accordance with the requirements of the Order and its implementing directives. Agencies 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.

(b) *Preparation of the exemptions files.* The Executive Secretary notifies the Chair of an agency's submission. At the direction of the ISCAP, the Executive Secretary supervises the preparation of an exemption file, pertinent portions of which are presented to the members of the Panel for review prior to a vote on the exemptions. The exemption file eventually includes all records pertaining to the ISCAP's consideration of the agency's exemptions.

(c) *Resolution.* The Panel 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 promptly notifies the designated senior agency official in writing of the Panel'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 National Security Advisor to overrule the Panel's decision.

(f) *Protection of classified information.* All persons involved in the appeal will make every effort to minimize the inclusion of classified information in the appeal file. Any classified information contained in the exemption file is handled and protected in accordance with the Order and its implementing directives. Information that the agency maintains is exempt from declassification remains classified unless and until a final decision is made to declassify it.

(g) *Maintenance and disposition of file.* The Executive Secretary maintains the exemption file among the ISCAP's records in accordance with 44 U.S.C. 2201–2207 (the Presidential Records Act).

§ 2003.13 Appeals of agency decisions denying declassification under mandatory review provisions in section 3.5 of the Order.

Section 3.5 of the Order requires agencies to conduct a mandatory declassification review, upon request, of classified information that meets the requirements set out in the Order. An agency may deny such a review for specific reasons set out in section 5.3(a) of the Order. If an agency denies a request for such review, a person may appeal the denial through the agency's appeal process. After that process, a person may further appeal to the ISCAP.

(a) *Jurisdiction.* The ISCAP considers and decides 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 procedures;

(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, and filed an appeal at the agency level. The request and appeal must have followed the agency's established procedures or, if the agency has failed to establish procedures, the appellant must have filed a written request directly with the agency head or designated senior agency official;

(3) The appellant has:

(i) Received a final agency decision denying his or her request; or

(ii) Not received—

(A) An initial decision on the request for mandatory declassification review from the agency within one year of its filing, or

(B) A final decision on an agency level 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;

(5) The information in question has not been the subject of an access review by the Federal courts or the ISCAP within the past two years; and

(6) The information in question is not the subject of a prepublication review or other administrative process pursuant to an approved nondisclosure agreement.

(b) *Submission of appeals.* Appeals may be submitted to the Panel by email or mail. Appeals should be sent via email to: *ISCAP@nara.gov* or by mail to: Executive Secretary, Interagency Security Classification Appeals Panel; Attn: Mandatory Declassification Review Appeals; c/o Information Security Oversight Office; National Archives and Records Administration; 700 Pennsylvania Avenue NW., Room 503; Washington, DC 20408.

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

(2) No classified information should be included within the initial appeal correspondence. 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 Panel in one of the two methods listed above.

(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)(i) and (ii) of this section.

(d) *Rejection of appeals.* If the Executive Secretary determines that an appeal does not meet the requirements of the Order or these bylaws, the Executive Secretary notifies the appellant in writing that the appeal will not be considered by the ISCAP. The notification includes an explanation of why the appeal is deficient.

(e) *Preparation of appeals and creation of appeals files.* The Executive Secretary notifies the senior agency official or primary member, alternate, or liaison of the affected agency(ies) when an appeal is lodged. Under the direction of the ISCAP, the Executive Secretary supervises the preparation of an appeal file, pertinent portions of which are presented to the members of the Panel for review prior to a vote on the appeal. The appeal file eventually includes all records pertaining to the appeal.

(f) *Narrowing appeals.* To expedite the resolution of appeals and minimize backlogs, the Executive Secretary consults as relevant with appellants and agencies to narrow or prioritize the information subject to the appeal.

(g) *Resolution of appeals.* The Panel 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. In circumstances in which members abstain from voting, a Panel decision to reverse an agency's classification decision requires the affirmative vote of at least a majority of the members present.

(h) *Notification.* The Executive Secretary promptly notifies the appellant and designated senior agency official in writing of the Panel'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 National Security Advisor to overrule the Panel's decision.

(j) *Protection of classified information.* All persons involved in the appeal will make every effort to minimize the inclusion of classified information in the appeal file. Any classified information contained in the appeal file is 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 remains classified unless and until a final decision is made to declassify it.

(k) *Maintenance and disposition of file.* The Executive Secretary shall maintain the appeal file among the ISCAP's records in accordance with 44 U.S.C. 2201–2207 (Presidential Records Act).

§ 2003.14 Dissemination of ISCAP decisions.

The Executive Secretary informs senior agency officials and the public of final ISCAP decisions on appeals under sections 1.8 and 3.5 of the Order.

§ 2003.15 Additional functions.

As directed by the President through the National Security Advisor, the ISCAP performs such additional advisory functions as are consistent with, and supportive of, the successful implementation of the Order.

PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

Subpart A—Implementation and Oversight

Subpart B—Administration

Subpart C—Operations

AUTHORITY: Section 102(b)(1) of E.O. 12829 (January 6, 1993), as amended by E.O. 12885 (December 14, 1993), E.O. 13691 (February 12, 2015), and section 4 of E.O. 13708 (September 30, 2015).

SOURCE: 83 FR 19951, May 7, 2018, unless otherwise noted.

Subpart A—Implementation and Oversight

§ 2004.1 Purpose and scope.

(a) This part sets out the National Industrial Security Program (''NISP'' or ''the Program'') governing the protection of agency classified information released to Federal contractors, licensees, grantees, and certificate holders. It establishes uniform standards throughout the Program, and helps agencies implement requirements in E.O. 12829, National Industrial Security Program, as amended by E.O. 12558 and E.O.13691 (collectively referred to as ''E.O. 12829''), E.O. 13691, Promoting Private Sector Cybersecurity Information Sharing, and E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. It applies to any executive branch agency that releases classified information to current, prospective, or former Federal contractors, licensees, grantees, or certificate holders. However, this part does not stand alone; users should refer concurrently to the underlying executive orders for guidance. ISOO maintains policy oversight over the NISP as established by E.O.12829.

(b) This part also does not apply to release of classified information pursuant to criminal proceedings. The Classified Information Procedures Act (CIPA) (18 U.S.C. Appendix 3) governs release of classified information in criminal proceedings.

(c) Nothing in this part supersedes the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, *et seq.*) (collectively referred to as ''the Atomic Energy Act''); the authority of the Director of National Intelligence (or any intelligence community element) under the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458), the National Security Act of 1947 as amended (50 U.S.C. 401, *et seq.*), and E.O. 12333 (December 4, 1981), as amended by E.O. 13355, Strengthened Management of the Intelligence Community (August 27, 2004) and E.O. 13470, Further Amendments to Executive Order 12333 (July 30, 2008) (collectively

referred to as ''E.O. 12333''); or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under E.O. 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities (August 18, 2010), or as established by E.O. 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security (January 23, 2003). In exercising these authorities, CSAs make every effort to facilitate reciprocity, avoid duplication of regulatory requirements, and facilitate uniform standards.

§ 2004.4 Definitions that apply to this part.

(a) *Access* is the ability or opportunity to gain knowledge of classified information.

(b) *Agency(ies)* are any ''Executive agency'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102; and any other entity within the executive branch that releases classified information to private sector entities. This includes component agencies under another agency or under a cross-agency oversight office (such as ODNI with CIA), which are also agencies for purposes of this regulation.

(c) *Classified Critical Infrastructure Protection Program (CCIPP)* is the DHS program that executes the classified infrastructure protection program designated by E.O. 13691, ''Promoting Private Sector Cybersecurity Information Sharing.'' The Government uses this program to share classified cybersecurity-related information with employees of private sector entities that own or operate critical infrastructure. Critical infrastructure refers to systems and assets, whether physical or virtual, so vital to the United States that incapacitating or destroying such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. These entities include banks and power plants, among others. The sectors of critical infrastructure are listed in Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (February 12, 2013).

(d) *Classified Critical Infrastructure Protection Program (CCIPP) security point of contact (security POC)* is an official whom a CCIPP entity designates to maintain eligibility information about the entity and its cleared employees, and to report that information to DHS. The CCIPP security POC must be eligible for access to classified information.

(e) *Classified information* is information the Government designates as requiring protection against unauthorized disclosure in the interest of national security, pursuant to E.O. 13526, Classified National Security Information, or any predecessor order, and the Atomic Energy Act of 1954, as amended. Classified information includes national security information (NSI), restricted data (RD), and formerly restricted data (FRD), regardless of its physical form or characteristics (including tangible items other than documents).

(f) *Cognizance* is the area over which a CSA has operational oversight. Normally, a statute or executive order establishes a CSA's cognizance over certain types of information, programs, or non-CSA agencies, although CSAs may also have cognizance through an agreement with another CSA or non-CSA agency or an entity. A CSA may have cognizance over a particular type(s) of classified information based on specific authorities (such as those listed in § 2004.1(c)), and a CSA may have cognizance over certain agencies or cross-agency programs (such as DoD's cognizance over non-CSA agencies as the EA for NISP, or ODNI's oversight (if applicable) of all intelligence community elements within the executive branch). Entities fall under a CSA's cognizance when they enter or compete to enter contracts or agreements to access classified information under the CSA's cognizance, including when they enter or compete to enter such contracts or agreements with a non-CSA agency or another entity under the CSA's cognizance.

(g) *Cognizant security agencies (CSAs)* are the agencies E.O. 12829, sec. 202, designates as having NISP implementation and security responsibilities for

their own agencies (including component agencies) and any entities and non-CSA agencies under their cognizance. The CSAs are: Department of Defense (DoD); Department of Energy (DOE); Nuclear Regulatory Commission (NRC); Office of the Director of National Intelligence (ODNI); and Department of Homeland Security (DHS).

(h) *Cognizant security office (CSO)* is an organizational unit to which the head of a CSA delegates authority to administer industrial security services on behalf of the CSA.

(i) *Contracts or agreements* are any type of arrangement between an agency and an entity or an agency and another agency. They include, but are not limited to, contracts, sub-contracts, licenses, certificates, memoranda of understanding, inter-agency service agreements, other types of documents or arrangements setting out responsibilities, requirements, or terms agreed upon by the parties, programs, projects, and other legitimate U.S. or foreign government requirements. FOCI mitigation or negation measures, such as Voting Trust Agreements, that have the word ''agreement'' in their title are not included in the term ''agreements'' within this part.

(j) *Controlling agency* is an agency that owns or controls the following categories of proscribed information and thus has authority over access to or release of the information: NSA for communications security information (COMSEC); DOE for restricted data (RD); and ODNI for sensitive compartmented information (SCI).

(k) *Entity* is a generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity (referred to as ''sub-entities'' when necessary to distinguish such entities from prime or parent entities), a specific location or facility, or the headquarters/official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible CSA's procedures. The term ''entity'' as used in this part refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or subordinate organization.

(l) *Entity eligibility determination* is an assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity would be accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs must also assess whether the entity is eligible for access to that category. Some CSAs refer to their favorable determinations as facility security clearances (FCL). A favorable entity eligibility determination does not convey authority to store classified information.

(m) *Foreign interest* is any foreign government, element of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the United States or its territories; and any person who is not a United States citizen or national.

(n) *Government contracting activity (GCA)* is an agency component or subcomponent to which the agency head delegates broad authority regarding acquisition functions. A foreign government may also be a GCA.

(o) *Industrial security services* are those activities performed by a CSA to verify that an entity is protecting classified information. They include, but

are not limited to, conducting oversight reviews, making eligibility determinations, and providing agency and entity guidance and training.

(p) *Insider(s)* are entity employees who are eligible to access classified information and may be authorized access to any U.S. Government or entity resource (such as personnel, facilities, information, equipment, networks, or systems).

(q) *Insider threat* is the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to entity or program information to the extent that the information impacts the entity's or agency's obligations to protect classified information.

(r) *Insider threat response action(s)* are actions (such as investigations) an agency takes to ascertain whether an insider threat exists, and actions the agency takes to mitigate the threat. Agencies may conduct insider threat response actions through their counterintelligence (CI), security, law enforcement, or inspector general organizations, depending on the statutory authority and internal policies that govern the agency.

(s) *Insider threat program senior official (SO)* is the official an agency head or entity designates with responsibility to manage, account for, and oversee the agency's or entity's insider threat program, pursuant to the National Insider Threat Policy and Minimum Standards. An agency may have more than one insider threat program SO.

(t) *Key managers and officials (KMO)* are the senior management official (or authorized executive official under CCIPP), the entity's security officer (or security POC under CCIPP), the insider threat program senior official, and other entity employees whom the responsible CSA identifies as having authority, direct or indirect, to influence or decide matters affecting the entity's management or operations, its contracts requiring access to classified information, or national security interests. They may include individuals who hold majority ownership interest in the entity (in the form of stock or other ownership interests).

(u) *Proscribed information* is information that is classified as top secret (TS) information; communications security (COMSEC) information (excluding controlled cryptographic items when unkeyed or utilized with unclassified keys); restricted data (RD); special access program information (SAP); or sensitive compartmented information (SCI).

(v) *Security officer* is a U.S. citizen employee the entity designates to supervise and direct security measures implementing NISPOM (or equivalent; such as DOE Orders) requirements. Some CSAs refer to this position as a facility security officer (FSO). The security officer must complete security training specified by the responsible CSA, and must have and maintain an employee eligibility determination level that is at least the same level as the entity's eligibility determination level.

(w) *Senior agency official for NISP (SAO for NISP)* is the official an agency head designates to direct and administer the agency's National Industrial Security Program.

(x) *Senior management official (SMO)* is the person in charge of an entity. Under the CCIPP, this is the authorized executive official with authority to sign the security agreement with DHS.

(y) *Sub-entity* is an entity's branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity. Sub-entities fall under the definition of ''entity,'' but this part refers to them as sub-entities when necessary to distinguish such entities from prime contractor or parent entities. See definition of ''entity'' in paragraph (k) of this section for more context.

§ 2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO).

The Director, ISOO:

(a) Implements E.O. 12829, including ensuring that:

(1) The NISP operates as a single, integrated program across the executive branch of the Federal Government (*i.e.*, such that agencies that release classified information to entities adhere to NISP principles);

(2) A responsible CSA oversees each entity's NISP implementation in accordance with § 2004.22;

(3) All agencies that contract for classified work include the Security Requirements clause, 48 CFR 52.204–2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in contracts that require access to classified information;

(4) Those agencies for which the Department of Defense (DoD) serves as the CSA or provides industrial security services have agreements with DoD defining the Secretary of Defense's responsibilities on behalf of their agency;

(5) Each CSA issues directions to entities under their cognizance that are consistent with the NISPOM insider threat guidance;

(6) CSAs share with each other, as lawful and appropriate, relevant information about entity employees that indicates an insider threat; and

(7) CSAs conduct ongoing analysis and adjudication of adverse or relevant information about entity employees that indicates an insider threat.

(b) Raises an issue to the National Security Council (NSC) for resolution if the EA's NISPOM coordination process cannot reach a consensus on NISPOM security standards (see § 2004.20(d)).

§ 2004.11 CSA and agency implementing regulations, internal rules, or guidelines.

(a) Each CSA implements NISP practices in part through policies and guidelines that are consistent with this regulation, so that agencies for which it serves as the CSA are aware of appropriate security standards, engage in consistent practices with entities, and so that practices effectively protect classified information those entities receive (including foreign government information that the U.S. Government must protect in the interest of national security).

(b) Each CSA must also routinely review and update its NISP policies and guidelines and promptly issue revisions when needed (including when a change in national policy necessitates a change in agency NISP policies and guidelines).

(c) Non-CSA agencies may choose to augment CSA NISP policies or guidelines as long as the agency policies or guidelines are consistent with the CSA's policies or guidelines and this regulation.

§ 2004.12 ISOO review of agency NISP implementation.

(a) ISOO fulfills its oversight role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the authority of E.O. 12829, and from any submitted complaints and suggestions. ISOO reports findings to the responsible CSA or agency.

(b) ISOO reviews agency policies and guidelines to ensure consistency with NISP policies and procedures. ISOO may conduct reviews during routine oversight visits, when a problem or potential problem comes to ISOO's attention, or after a change in national policy that impacts agency policies and guidelines. ISOO provides the responsible agency with findings from these reviews.

Subpart B—Administration

§ 2004.20 National Industrial Security Program Executive Agent and Operating Manual.

(a) The executive agent (EA) for NISP is the Secretary of Defense. The EA:

(1) Provides industrial security services for agencies that are not CSAs but that release classified information to entities. The EA provides industrial security services only through an agreement with the agency. Non-CSA agencies must enter an agreement with the EA and comply with EA industrial security service processes before releasing classified information to an entity;

(2) Provides services for other CSAs by agreement; and

(3) Issues and maintains the National Industrial Security Program Operating Manual (NISPOM) in consultation with all affected agencies and with the concurrence of the other CSAs.

(b) The NISPOM sets out the procedures and standards that entities must

follow during all phases of the contracting process to safeguard any classified information an agency releases to an entity. The NISPOM requirements may apply to the entity directly (*i.e.*, through FAR clauses or other contract clauses referring entities to the NISPOM) or through equivalent contract clauses or requirements documents that are consistent with NISPOM requirements.

(c) The EA, in consultation with all affected agencies and with the concurrence of the other CSAs, develops the requirements, restrictions, and safeguards contained in the NISPOM. The EA uses security standards applicable to agencies as the basis for developing NISPOM entity standards to the extent practicable and reasonable.

(d) The EA also facilitates the NISPOM coordination process, which addresses issues raised by entities, agencies, ISOO, or the NISPPAC, including requests to create or change NISPOM security standards.

§ 2004.22 Agency responsibilities.

(a) *Agency categories and general areas of responsibility*. Federal agencies fall into three categories for the purpose of NISP responsibilities:

(1) *CSAs*. CSAs are responsible for carrying out NISP implementation within their agency, for providing NISP industrial security services on behalf of non-CSA agencies by agreement when authorized, and for overseeing NISP compliance by entities that access classified information under the CSA's cognizance. When the CSA has oversight responsibilities for a particular non-CSA agency or for an entity, the CSA also functions as the responsible CSA;

(2) *Non-CSA agencies*. Non-CSA agencies are responsible for entering agreements with a designated CSA for industrial security services, and are responsible for carrying out NISP implementation within their agency consistently with the agreement, the CSA's guidelines and procedures, and this regulation; or

(3) *Agencies that are components of another agency*. Component agencies do not have itemized responsibilities under this regulation and do not independently need to enter agreements with a CSA, but they follow, and may have responsibilities under, implementing guidelines and procedures established by their CSA or non-CSA agency, or both.

(b) *Responsible CSA role*. (1) The responsible CSA is the CSA (or its delegated CSO) that provides NISP industrial security services on behalf of an agency, determines an entity's eligibility for access, and monitors and inspects an entity's NISP implementation.

(2) In general, the goal is to have one responsible CSA for each agency and for each entity, to minimize the burdens that can result from complying with differing CSA procedures and requirements.

(i) With regard to agencies, NISP accomplishes this goal by a combination of designated CSAs and agreements between agencies and CSAs.

(ii) With regard to entities, CSAs strive to reduce the number of responsible CSAs for a given entity as much as possible. To this end, when more than one CSA releases classified information to a given entity, those CSAs agree on which is the responsible CSA. However, due to certain unique agency authorities, there may be circumstances in which a given entity is under the oversight of more than one responsible CSA.

(3) Responsible CSA for agencies:

(i) In general, each CSA serves as the responsible CSA for classified information that it (or any of its component agencies) releases to entities, unless it enters an agreement otherwise with another CSA.

(ii) DoD serves as the responsible CSA for DHS with the exception of the CCIPP, based on an agreement between the two CSAs.

(iii) DoD serves as the responsible CSA on behalf of all non-CSA agencies, except CSA components, based on E.O. 12829 and its role as NISP EA.

(iv) ODNI serves as the responsible CSA for CIA.

(4) Responsible CSA for entities: When determining the responsible CSA for a given entity, the involved CSAs

consider, at a minimum: retained authorities, the information's classification level, number of contracts requiring access to classified information, location, number of Government customers, volume of classified activity, safeguarding requirements, responsibility for entity employee eligibility determinations, and any special requirements.

(5) Responsible CSAs may delegate oversight responsibility to a cognizant security office (CSO) through CSA policy or by written delegation. The CSA must inform entities under its cognizance if it delegates responsibilities. For purposes of this rule, the term CSA also refers to the CSO.

(c) *CSA responsibilities.* (1) The CSA may perform GCA responsibilities as its own GCA.

(2) As CSA, the CSA performs or delegates the following responsibilities:

(i) Designates a CSA senior agency official (SAO) for NISP;

(ii) Identifies the insider threat program senior official (SO) to the Director, ISOO;

(iii) Shares insider threat information with other CSAs, as lawful and appropriate, including information that indicates an insider threat about entity employees eligible to access classified information;

(iv) Acts upon and shares—with security management, GCAs, insider threat program employees, and Government program and CI officials—any relevant entity-reported information about security or CI concerns, as appropriate;

(v) Submits reports to ISOO as required by this part; and

(vi) Develops, coordinates, and provides concurrence on changes to the NISPOM when requested by the EA.

(3) As a responsible CSA, the CSA also performs or delegates the following responsibilities:

(i) Determines whether an entity is eligible for access to classified information (see § 2004.32);

(ii) Allocates funds, ensures appropriate investigations are conducted, and determines entity employee eligibility for access to classified information (see § 2004.36);

(iii) Reviews and approves entity safeguarding measures, including making safeguarding capability determinations (see § 2004.38);

(iv) Conducts periodic security reviews of entity operations (see § 2004.26) to determine that entities: effectively protect classified information provided to them; and follow NISPOM (or equivalent) requirements;

(v) Provides and regularly updates guidance, training, training materials, and briefings to entities on:

(A) Entity implementation of NISPOM (or equivalent) requirements, including: responsibility for protecting classified information, requesting NISPOM interpretations, establishing training programs, and submitting required reports;

(B) Initial security briefings and other briefings required for special categories of information;

(C) Authorization measures for information systems processing classified information (except DHS) (see § 2004.40);

(D) Security training for security officers (or CCIPP POCs) and other employees whose official duties include performing NISP-related functions;

(E) Insider threat programs in accordance with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and

(F) Other guidance and training as appropriate;

(vi) Establishes a mechanism for entities to submit requests for waivers to NISPOM (or equivalent) provisions;

(vii) Reviews, continuously analyzes, and adjudicates, as appropriate, reports from entities regarding events that:

(A) Impact the status of the entity's eligibility for access to classisfied information;

(B) Impact an employee's eligibility for access;

(C) May indicate an employee poses an insider threat;

(D) Affect proper safeguarding of classified information; or

(E) Indicate that classified information has been lost or compromised;

(viii) Verifies that reports offered in confidence and so marked by an entity may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552);

(ix) Requests any additional information needed from an entity about involved employees to determine continued eligibility for access to classified information when the entity reports loss, possible compromise, or unauthorized disclosure of classified information; and

(x) Posts hotline information on its website for entity access, or otherwise disseminates contact numbers to the entities for which the CSA is responsible.

(d) *Non-CSA agency head responsibilities*. The head of a non-CSA agency that is not a CSA component and that releases classified information to entities, performs the following responsibilities:

(1) Designates an SAO for the NISP;

(2) Identifies the insider threat program SO to ISOO to facilitate information sharing;

(3) Enters into an agreement with the EA (except agencies that are components of another agency or a cross-agency oversight office) to act as the responsible CSA on the agency's behalf (see paragraph (a)(1)(ii) of this section);

(4) Performs, or delegates in writing to a GCA, the following responsibilities:

(i) Provides appropriate education and training to agency personnel who implement the NISP;

(ii) Includes FAR security requirements clause 52.204–2, or equivalent (such as the DEAR clause 952.204–2), and a contract security classification specification (or equivalent guidance) into contracts and solicitations that require access to classified information (see § 2004.30); and

(iii) Reports to the appropriate CSA adverse information and insider threat activity pertaining to entity employees having access to classified information.

§ 2004.24 Insider threat program.

(a) Responsible CSAs oversee and analyze entity activity to ensure entities implement an insider threat program in accordance with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (via requirements in the NISPOM or its equivalent) and guidance from the CSA. CSA oversight responsibilities include, but are not limited to:

(1) Verifying that entities appoint insider threat program SOs;

(2) Requiring entities to monitor, report, and review insider threat program activities and response actions in accordance with the provisions set forth in the NISPOM (or equivalent);

(3) Providing entities with access to data relevant to insider threat program activities and applicable reporting requirements and procedures;

(4) Providing entities with a designated means to report insider threat-related activity; and

(5) Advising entities on appropriate insider threat training for entity employees eligible for access to classified information.

(b) CSAs share with other CSAs any insider threat information reported to them by entities, as lawful and appropriate.

§ 2004.26 Reviews of entity NISP implementation.

(a) The responsible CSA conducts recurring oversight reviews of entities' NISP security programs to verify that the entity is protecting classified information and is implementing the provisions of the NISPOM (or equivalent). The CSA determines the scope and frequency of reviews. The CSA generally notifies entities when a review will take place, but may also conduct unannounced reviews at its discretion.

(b) CSAs make every effort to avoid unnecessarily intruding into entity employee personal effects during the reviews.

(c) A CSA may, on entity premises, physically examine the interior spaces of containers not authorized to store classified information in the presence of the entity's representative.

(d) As part of a security review, the CSA:

(1) Verifies that the entity limits entity employees with access to classified information to the minimum number necessary to perform on contracts requiring access to classified information.

(2) Validates that the entity has not provided its employees unauthorized access to classified information;

(3) Reviews the entity's self-inspection program and evaluates and records the entity's remedial actions; and

(4) Verifies that the GCA approved any public release of information pertaining to a contract requiring access to classified information.

(e) As a result of findings during the security review, the CSA may, as appropriate, notify:

(1) GCAs if there are unfavorable results from the review; and

(2) A prime entity if the CSA discovers unsatisfactory security conditions pertaining to a sub-entity.

(f) The CSA maintains a record of reviews it conducts and the results. Based on review results, the responsible CSA determines whether an entity's eligibility for access to classified information may continue. See § 2004.32(g).

§ 2004.28 Cost reports.

(a) Agencies must annually report to the Director, ISOO, on their NISP implementation costs for the previous year.

(b) CSAs must annually collect information on NISP implementation costs incurred by entities under their cognizance and submit a report to the Director, ISOO.

Subpart C—Operations

§ 2004.30 Security classification requirements and guidance.

(a) *Contract or agreement and solicition requirements.* (1) The GCA must incorporate FAR clause 52.204–2, Security Requirements (or equivalent set of security requirements), into contracts or agreements and solicitations requiring access to classified information.

(2) The GCA must also include a contract security classification specification (or equivalent guidance) with each contract or agreement and solicitation that requires access to classified information. The contract security classification specification (or equivalent guidance) must identify the specific elements of classified information involved in each phase of the contract or agreement life-cycle, such as:

(i) Level of classification;

(ii) Where the entity will access or store the classified information, and any requirements or limitations on transmitting classified information outside the entity;

(iii) Any special accesses;

(iv) Any classification guides or other guidance the entity needs to perform during that phase of the contract or agreement;

(v) Any authorization to disclose information about the contract or agreement requiring access to classified information; and

(vi) GCA personnel responsible for interpreting and applying the contract security specifications (or equivalent guidance).

(3) The GCA revises the contract security classification specification (or equivalent guidance) throughout the contract or agreement life-cycle as security requirements change.

(b) *Guidance.* Classification guidance is the exclusive responsibility of the GCA. The GCA prepares classification guidance in accordance with 32 CFR 2001.15, and provides appropriate security classification and declassification guidance to entities.

(c) *Requests for clarification and classification challenges.* (1) The GCA responds to entity requests for clarification and classification challenges.

(2) The responsible CSA assists entities to obtain appropriate classification guidance from the GCA, and to obtain a classification challenge response from the GCA.

(d) *Instructions upon contract or agreement completion or termination.* (1) The GCA provides instructions to the entity for returning or disposing of classified information upon contract or agreement completion or termination, or when an entity no longer has a legitimate need to retain or possess classified information.

(2) The GCA also determines whether the entity may retain classified information for particular purposes after the contract or agreement terminates, and if so, provides written authorization to the entity along with any instructions or limitations (such as which information, for how long, etc).

§ 2004.32 Determining entity eligibility for access to classified information.

(a) *Eligibility determinations.* (1) The responsible CSA determines whether an

entity is eligible for access to classified information. An entity may not have access to classified information until the responsible CSA determines that it meets all the requirements in this section. In general, the entity must be eligible to access classified information at the appropriate level before the CSA may consider any of the entity's subsidiaries, sub-contractors, or other subentities for eligibility. However, when the subsidiary will perform all classified work, the CSA may instead exclude the parent entity from access to classified information rather than determining its eligibility. In either case, the CSA must consider all information relevant to assessing whether the entity's access poses an unacceptable risk to national security interests.

(2) A favorable access eligibility determination is not the same as a safeguarding capability determination. Entities may access classified information with a favorable eligibility determination, but may possess classified information only if the CSA determines both access eligibility and safeguarding capability, based on the GCA's requirement in the contract security classification specification (or equivalent).

(3) If an entity has an existing eligibility determination, a CSA will not duplicate eligibility determination processes performed by another CSA. If a CSA cannot acknowledge an entity eligibility determination to another CSA, that entity may be subject to duplicate processing.

(4) Each CSA maintains a record of its entities' eligibility determinations (or critical infrastructure entity eligibility status under the CCIPP, for DHS) and responds to inquiries from GCAs or entities, as appropriate and to the extent authorized by law, regarding the eligibility status of entities under their cognizance.

(b) *Process.* (1) The responsible CSA provides guidance to entities on the eligibility determination process and on how to maintain eligibility throughout the period of the agreement or as long as an entity continues to need access to classified information in connection with a legitimate U.S. or foreign government requirement.

(2) The CSA coordinates with appropriate authorities to determine whether an entity meets the eligibility criteria in paragraph (e) of this section. This includes coordinating with appropriate U.S. Government regulatory authorities to determine entity compliance with laws and regulations.

(3) An entity cannot apply for its own eligibility determination. A GCA or an eligible entity must sponsor the entity to the responsible CSA for an eligibility determination. The GCA or eligible entity may sponsor an entity at any point during the contracting or agreement life-cycle at which the entity must have access to classified information to participate (including the solicitation or competition phase). An entity with limited eligibility granted under paragraph (f) of this section may sponsor a sub-entity for a limited eligibility determination for the same contract, agreement, or circumstance so long as the sponsoring entity is not under FOCI (see § 2004.34(i)).

(4) The GCA must include enough lead time in each phase of the acquisition or agreement cycle to accomplish all required security actions. Required security actions include any eligibility determination necessary for an entity to participate in that phase of the cycle. The GCA may award a contract or agreement before the CSA completes the entity eligibility determination. However, in such cases, the entity may not begin performance on portions of the contract or agreement that require access to classified information until the CSA makes a favorable entity eligibility determination.

(5) When a CSA is unable to make an eligibility determination in sufficient time to qualify an entity to participate in the particular procurement action or phase that gave rise to the GCA request (this includes both solicitation and performance phases), the GCA may request that the CSA continue the determination process to qualify the entity for future classified work for any GCA, provided that the processing delay was not due to the entity's lack of cooperation. Once the CSA determines that an entity is eligible for access to classified information, but a GCA does not award a contract or

agreement requiring access to classified information to the entity, or the entity's eligibility status changes, the CSA terminates the entity eligibility determination in accordance with paragraph (g) of this section.

(c) *Coverage.* (1) A favorable eligibility determination allows an entity to access classified information at the determined eligibility level, or lower.

(2) The CSA must ensure that all entities needing access to classified information as part of a legitimate U.S. or foreign government requirement have or receive a favorable eligibility determination before accessing classified information. This includes both prime or parent entities and sub-entities, even in cases in which an entity intends to have the classified work performed only by sub-entities. A prime or parent entity must have a favorable eligibility determination at the same classification level or higher than its sub-entity(ies), unless the CSA determined that the parent entity could be effectively excluded from access (see paragraph (a)(1) of this section).

(3) If a parent and sub-entity need to share classified information with each other, the CSA must validate that both the parent and the sub-entity have favorable eligibility determinations at the level required for the classified information prior to sharing the information.

(d) *DHS Classified Critical Infrastructure Protection Program (CCIPP).* DHS shares classified cybersecurity information with certain employees of entities under the Classified Critical Infrastructure Protection Program (CCIPP). The CCIPP applies only to entities that do not need to store classified information, have no other contracts or agreements already requiring access to classified information, and are not already determined eligible for access to classified information. DHS establishes and implements procedures consistent with the NISP to determine CCIPP entity eligibility for access to classified information.

(e) *Eligibility criteria.* An entity must meet the following requirements to be eligible to access classified information:

(1) It must need to access classified information as part of a legitimate U.S. Government or foreign government requirement, and access must be consistent with U.S. national security interests as determined by the CSA;

(2) It must be organized and existing under the laws of any of the 50 States, the District of Columbia, or an organized U.S. territory (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands); or an American Indian or Alaska native tribe formally acknowledged by the Assistant Secretary—Indian Affairs, of the U.S. Department of the Interior;

(3) It must be located in the United States or its territorial areas;

(4) It must have a record of compliance with pertinent laws, regulations, and contracts (or other relevant agreements);

(5) Its KMOs must each have and maintain eligibility for access to classified information that is at least the same level as the entity eligibility level;

(6) It and all of its KMOs must not be excluded by a Federal agency, contract review board, or other authorized official from participating in Federal contracts or agreements;

(7) It must meet all requirements the CSA or the authorizing law, regulation, or Government-wide policy establishes for access to the type of classified information or program involved; and

(8) If the CSA determines the entity is under foreign ownership, control, or influence (FOCI), the responsible CSA must:

(i) Agree that sufficient security measures are in place to mitigate or negate risk to national security interests due to the FOCI (see § 2004.34);

(ii) Determine that it is appropriate to grant eligibility for a single, narrowly defined purpose (see § 2004.34(i)); or

(iii) Determine that the entity is not eligible to access classified information.

(9) DoD and DOE cannot award a contract involving access to proscribed information to an entity effectively owned or controlled by a foreign government unless the Secretary of the agency first issues a waiver (see 10 U.S.C. 2536). A waiver is not required if

the CSA determines the entity is eligible and it agrees to establish a voting trust agreement (VTA) or proxy agreement (PA) (see § 2004.34(f)) because both VTAs and PAs effectively negate foreign government control.

(f) *Limited entity eligibility determination.* CSAs may choose to allow GCAs to request limited entity eligibility determinations (this is not the same as limited entity eligibility in situations involving FOCI when the FOCI is not mitigated or negated; for more information on limited entity eligibility in such FOCI cases, see § 2004.34(i)). If a CSA permits GCAs to request a limited entity eligibility determination, it must set out parameters within its implementing policies that are consistent with the following requirements:

(1) The GCA, or an entity with limited eligibility, must first request a limited entity eligibility determination from the CSA for the relevant entity and provide justification for limiting eligibility in that case;

(2) Limited entity eligibility is specific to the requesting GCA's classified information, and to a single, narrowly defined contract, agreement, or circumstance;

(3) The entity must otherwise meet the requirements for entity eligibility set out in this part;

(4) The CSA documents the requirements of each limited entity eligibility determination it makes, including the scope of, and any limitations on, access to classified information;

(5) The CSA verifies limited entity eligibility determinations only to the requesting GCA or entity. In the case of multiple limited entity eligibility determinations for a single entity, the CSA verifies each one separately only to its requestor; and

(6) CSAs administratively terminate the limited entity eligibility when there is no longer a need for access to the classified information for which the CSA approved the limited entity eligibility.

(g) *Terminating or revoking eligibility.* (1) The responsible CSA terminates the entity's eligible status when the entity no longer has a need for access to classified information.

(2) The responsible CSA revokes the entity's eligible status if the entity is unable or unwilling to protect classified information.

(3) The CSA coordinates with the GCA(s) to take interim measures, as necessary, toward either termination or revocation.

§ 2004.34 Foreign ownership, control, or influence (FOCI).

(a) *FOCI determination.* A U.S. entity is under foreign ownership, control, or influence (FOCI) when:

(1) A foreign interest has the power to direct or decide matters affecting the entity's management or operations in a manner that could:

(i) Result in unauthorized access to classified information; or

(ii) Adversely affect performance of a contract or agreement requiring access to classified information; and

(2) The foreign interest exercises that power:

(i) Directly or indirectly;

(ii) Through ownership of the U.S. entity's securities, by contractual arrangements, or other similar means;

(iii) By the ability to control or influence the election or appointment of one or more members to the entity's governing board (*e.g.,* board of directors, board of managers, board of trustees) or its equivalent; or

(iv) Prospectively (*i.e.,* is not currently exercising the power, but could).

(b) *CSA guidance.* The CSA establishes guidance for entities on filling out and submitting a Standard Form (SF) 328, Certificate Pertaining to Foreign Interests (OMB Control No. 0704–0194), and on reporting changes in circumstances that might result in a determination that the entity is under FOCI or is no longer under FOCI. The CSA also advises entities on the Government appeal channels for disputing CSA FOCI determinations.

(c) *FOCI factors.* To determine whether an entity is under FOCI, the CSA analyzes available information to determine the existence, nature, and source of FOCI. The CSA:

(1) Considers information the entity or its parent provides on the SF 328/CF 328 (OMB Control No. 0704–0194), and any other relevant information; and

(2) Considers in the aggregate the following factors about the entity:

(i) Record of espionage against U.S. targets, either economic or Government;

(ii) Record of enforcement actions against the entity for transferring technology without authorization;

(iii) Record of compliance with pertinent U.S. laws, regulations, and contracts or agreements;

(iv) Type and sensitivity of the information the entity would access;

(v) Source, nature, and extent of FOCI, including whether foreign interests hold a majority or minority position in the entity, taking into consideration the immediate, intermediate, and ultimate parent entities;

(vi) Nature of any relevant bilateral and multilateral security and information exchange agreements;

(vii) Ownership or control, in whole or in part, by a foreign government; and

(viii) Any other factor that indicates or demonstrates foreign interest capability to control or influence the entity's operations or management.

(d) *Entity access while under FOCI.* (1) If the CSA is determining whether an entity is eligible to access classified information and finds that the entity is under FOCI, the CSA must consider the entity ineligible for access to classified information. The CSA and the entity may then attempt to negotiate FOCI mitigation or negation measures sufficient to permit a favorable eligibility determination.

(2) The CSA may not determine that the entity is eligible to access classified information until the entity has put into place appropriate security measures to negate or mitigate FOCI or is otherwise no longer under FOCI. If the degree of FOCI is such that no mitigation or negation efforts will be sufficient, or access to classified information would be inconsistent with national security interests, then the CSA will determine the entity ineligible for access to classified information.

(3) If an entity comes under FOCI, the CSA may allow the existing eligibility status to continue while the CSA and the entity negotiate acceptable FOCI mitigation or negation measures, as long as there is no indication that classified information is at risk. If the entity does not actively negotiate mitigation or negation measures in good faith, or there are no appropriate measures that will remove the possibility of unauthorized access to classified information or adverse effect on the entity's performance of contracts or agreements involving classified information, the CSA will take steps, in coordination with the GCA, to terminate eligibility.

(e) *FOCI and entities under the CCIPP.* DHS may sponsor, as part of the CCIPP, a U.S. entity that is under FOCI, under the following circumstances:

(1) The Secretary of DHS proposes appropriate FOCI risk mitigation or negation measures (see paragraph (f) of this section) to the other CSAs and ensures the anticipated release of classified information:

(i) Is authorized for release to the country involved;

(ii) Does not include information classified under the Atomic Energy Act; and

(iii) Does not impede or interfere with the entity's ability to manage and comply with regulatory requirements imposed by other Federal agencies, such as the State Department's International Traffic in Arms Regulation.

(2) If the CSAs agree the mitigation or negation measures are sufficient, DHS may proceed to enter a CCIPP information sharing agreement with the entity. If one or more CSAs disagree, the Secretary of DHS may seek a decision from the Assistant to the President for National Security Affairs before entering a CCIPP information sharing agreement with the entity.

(f) *Mitigation or negation measures to address FOCI.* (1) The CSA-approved mitigation or negation measures must assure that the entity can offset FOCI by effectively denying unauthorized people or entities access to classified information and preventing the foreign interest from adversely impacting the entity's performance on contracts or agreements requiring access to classified information.

(2) Any mitigation or negation measures the CSA approves for an entity must not impede or interfere with the entity's ability to manage and comply with regulatory requirements imposed

by other Federal agencies (such as Department of State's International Traffic in Arms Regulation).

(3) If the CSA approves a FOCI mitigation or negation measure for an entity, it may agree that the measure, or particular portions of it, may apply to all of the present and future sub-entities within the entity's organization.

(4) Mitigation or negation measures are different for ownership versus control or influence.

(5) Methods to mitigate foreign control or influence (unrelated to ownership) may include:

(i) Assigning specific oversight duties and responsibilities to independent board members;

(ii) Formulating special executive-level security committees to consider and oversee matters that affect entity performance on contracts or agreements requiring access to classified information;

(iii) Modifying or terminating loan agreements, contracts, agreements, and other understandings with foreign interests;

(iv) Diversifying or reducing foreign-source income;

(v) Demonstrating financial viability independent of foreign interests;

(vi) Eliminating or resolving problem debt;

(vii) Separating, physically or organizationally, the entity component performing on contracts or agreements requiring access to classified information;

(viii) Adopting special board resolutions;

(ix) A combination of these methods, as determined by the CSA; or

(x) Other actions that effectively negate or mitigate foreign control or influence.

(6) Methods to mitigate or negate foreign ownership include:

(i) *Board resolutions.* The CSA and the entity may agree to a board resolution when a foreign interest does not own voting interests sufficient to elect, or is otherwise not entitled to representation on, the entity's governing board. The resolution must identify the foreign shareholders and their representatives (if any), note the extent of foreign ownership, certify that the foreign shareholders and their representatives will not require, will not have, and can be effectively excluded from, access to all classified information, and certify that the entity will not permit the foreign shareholders and their representatives to occupy positions that might enable them to influence the entity's policies and practices, affecting its performance on contracts or agreements requiring access to classified information.

(ii) *Security control agreements (SCAs).* The CSA and the entity may agree to use an SCA when a foreign interest does not effectively own or control an entity (*i.e.,* the entity is under U.S. control), but the foreign interest is entitled to representation on the entity's governing board. At least one cleared U.S. citizen must serve as an outside director on the entity's governing board.

(iii) *Special security agreements (SSAs).* The CSA and the entity may agree to use an SSA when a foreign interest effectively owns or controls an entity. The SSA preserves the foreign owner's right to be represented on the entity's board or governing body with a direct voice in the entity's business management, while denying the foreign owner majority representation and unauthorized access to classified information. When a GCA requires an entity to have access to proscribed information, and the CSA proposes an SSA as the mitigation measure, the CSA makes a national interest determination (NID) as part of determining an entity's eligibility for access. See paragraph (h) of this section for more information on NIDs.

(iv) *Voting trust agreements (VTAs) or proxy agreements (PAs).* The CSA and the entity may agree to use one of these measures when a foreign interest effectively owns or controls an entity. The VTA and PA are arrangements that vest the voting rights of the foreign-owned stock in cleared U.S. citizens approved by the CSA. Under the VTA, the foreign owner transfers legal title in the entity to the trustees approved by the CSA. Under the PA, the foreign owner conveys their voting rights to proxy holders approved by the CSA. The entity must be organized, structured, and financed to be capable of operating as a viable business entity

independently from the foreign owner. Both VTAs and PAs can effectively negate foreign ownership and control; therefore, neither imposes any restrictions on the entity's eligibility to have access to classified information or to compete for contracts or agreements requiring access to classified information, including those involving proscribed information. Both VTAs and PAs can also effectively negate foreign government control.

(v) *Combinations of the measures in paragraphs (f)(6)(i) through (iv) of this section or other similar measures that effectively mitigate or negate the risks involved with foreign ownership.* CSAs must identify combination agreements in a way that distinguishes them from other agreements (*e.g.*, a combination SSA-proxy agreement cannot be identified as either an SSA or a proxy agreement beause those names would not distinguish the combination agreement from either of the other types). CSAs must also coordinate terms in combination agreements with the controlling agency prior to releasing proscribed information.

(g) *Standards for FOCI mitigation or negation measures.* The CSA must include the following requirements as part of any FOCI mitigation or negation measures, to ensure that entities implement necessary security and governing controls:

(1) Annual certification and annual compliance reports by the entity's governing board and the KMOs;

(2) The U.S. Government remedies in case the entity is not adequately protecting classified information or not adhering to the provisions of the mitigation or negation measure;

(3) Supplements to FOCI mitigation or negation measures as the CSA deems necessary. In addition to the standard FOCI mitigation or negation measure's requirements, the CSA may require more procedures via a supplement, based upon the circumstances of an entity's operations. The CSA may place these requirements in supplements to the FOCI mitigation or negation measure to allow flexibility as circumstances change without having to renegotiate the entire measure. When making use of supplements, the CSA does not consider the FOCI mitigation measure final until it approves the required supplements (*e.g.*, technology control plan, electronic communication plan); and

(4) For agreements to mitigate or negate ownership (PAs, VTAs, SSAs, and SCAs), the following additional requirements apply:

(i) *FOCI oversight.* The CSA verifies that the entity establishes an oversight body consisting of trustees, proxy holders or outside directors, as applicable, and those officers or directors whom the CSA determines are eligible for access to classified information (see § 2004.36). The entity's security officer is the principal advisor to the oversight body and attends their meetings. The oversight body:

(A) Maintains policies and procedures to safeguard classified information in the entity's possession with no adverse impact on performance of contracts or agreements requiring access to classified information; and

(B) Verifies the entity is complying with the FOCI mitigation or negation measure and related documents, contract security requirements or equivalent, and the NISP;

(ii) *Qualifications of trustees, proxy holders, and outside directors.* The CSA determines eligibility for access to classified information for trustees, proxy holders, and outside directors at the classification level of the entity's eligibility determination. Trustees, proxy holders, and outside directors must meet the following criteria:

(A) Be a U.S. citizen residing in the United States who can exercise management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the entity or effectively separated from the entity's classified work;

(B) Be completely disinterested individuals with no prior involvement with the entity, the entities with which it is affiliated, or the foreign owner and its affiliates. Individuals who are serving as trustees, proxy holders, or outside directors as part of a mitigation measure for the entity are not considered to have prior involvement solely by performing that role; and

(C) Be involved in no other circumstances that may affect an individual's ability to serve effectively, such as the number of boards on which the individual serves or the length of time serving on any other boards;

(iii) *Annual meeting.* The CSA meets at least annually with the oversight body to review the purpose and effectiveness of the FOCI mitigation or negation agreement; establish a common understanding of the operating requirements and their implementation; and provide guidance on matters related to FOCI mitigation and industrial security. These meetings include a CSA review of:

(A) Compliance with the approved FOCI mitigation or negation measure;

(B) Problems regarding practical implementation of the mitigation or negation measure; and

(C) Security controls, practices, or procedures and whether they warrant adjustment; and

(iv) *Annual certification.* The CSA reviews the entity's annual report; addresses, and resolves issues identified in the report; and documents the results of this review and any follow-up actions.

(h) *National interest determination (NID)*—(1) *Requirement for a NID.* (i) The CSA must determine whether allowing an entity access to proscribed information under an SSA is consistent with national security interests of the United States as part of making an entity eligibility determination in cases in which:

(A) The GCA requires an entity to have access to proscribed information;

(B) The entity is under FOCI; and

(C) The CSA proposes an SSA to mitigate the FOCI.

(ii) This determination is called a national interest determination (NID). A favorable NID confirms that an entity's access to the proscribed information under an SSA is consistent with national security interests. If the CSA is unable to render a favorable NID, it must consider other FOCI mitigation measures instead of an SSA or reassess the entity's eligibility for access to classified information.

(2) *NID process.* (i) The CSA makes the NID for any categories of proscribed information for which the entity requires access.

(ii) In cases in which any category of the proscribed information is controlled by another agency (ODNI for SCI, DOE for RD, NSA for COMSEC), the CSA asks that controlling agency to concur on the NID for that category of information.

(iii) The CSA informs the GCA and the entity when the NID is complete. In cases involving SCI, RD, or COMSEC, the CSA also informs the GCA and the entity when a controlling agency concurs or non-concurs on that agency's category of proscribed information. The entity may begin accessing a category of proscribed information once the CSA informs the GCA and the entity that the controlling agency concurs, even if other categories of proscribed information are pending concurrence.

(iv) An entity's access to SCI, RD, or COMSEC remains in effect so long as the entity remains eligible for access to classified information and the contract or agreement (or program or project) which imposes the requirement for access to those categories of proscribed information remains in effect, except under the following circumstances:

(A) The CSA, GCA, or controlling agency becomes aware of adverse information that impacts the entity eligibility determination;

(B) The CSA's threat assessment pertaining to the entity indicates a risk to one of the categories of proscribed information;

(C) The CSA becomes aware of any material change regarding the source, nature, and extent of FOCI; or

(D) The entity's record of NISP compliance, based on CSA reviews in accordance with § 2004.26, becomes less than satisfactory.

(v) Under any of these circumstances, the CSA determines whether an entity may continue being eligible for access to classified information, it must change the FOCI mitigation measure in order to remain eligible, or the CSA must terminate or revoke access.

(3) *Process for concurring or non-concurring on a NID.* (i) Each controlling agency tells the CSAs what information the controlling agency requires to

consider a NID. ODNI identifies the information it requires to assess a NID for access to SCI, DOE identifies the information it requires to assess a NID for access to RD, and NSA identifies the information it requires to assess a NID for access to COMSEC.

(ii) The CSA requests from the GCA justification for access, a description of the proscribed information involved, and other information the controlling agency requires to concur or non-concur on the NID.

(iii) The CSA requests concurrence on the NID from the controlling agency for the relevant category of proscribed information (ODNI for SCI, DOE for RD, NSA for COMSEC), and provides the information that controlling agency identified.

(iv) The relevant controlling agency (ODNI for SCI, DOE for RD, NSA for COMSEC) responds in writing to the CSA's request for concurrence.

(A) The controlling agency may concur with the NID for access under a particular contract or agreement, access under a program or project, or for all future access to the same category of proscribed information.

(B) If the relevant controlling agency does not concur with the NID, the controlling agency informs the CSA in writing, citing the reasons why it does not concur. The CSA notifies the applicable GCA and, in coordination with the GCA, then notifies the entity. The entity cannot have access to the category of proscribed information under the control of that agency (*i.e.*, if ODNI does not concur, the entity may not have access to SCI; if DOE does not concur, the entity may not have access to RD; and if NSA does not concur, the entity may not have access to COMSEC). The CSA, in consultation with the applicable GCA, must decide whether the reason the controlling agency did not concur otherwise affects the entity's eligibility for access to classified information (see § 2004.32(g)), or requires changing the FOCI mitigation measure (see paragraph (f) of this section).

(v) When an entity is eligible for access to classified information that includes a favorable NID for SCI, RD, or COMSEC, the CSA does not have to request a new NID concurrence for the same entity if the access requirements for the relevant category of proscribed information and terms remain unchanged for:

(A) Renewing the contract or agreement;

(B) New task orders issued under the contract or agreement;

(C) A new contract or agreement that contains the same provisions as the previous one (this usually applies when the contract or agreement is for a program or project); or

(D) Renewing the SSA.

(vi) When making the decision whether or not to concur with a NID for proscribed information under its control, the controlling agency will not duplicate work already performed by the GCA during the contract award process or by the CSA when determining entity eligibility for access to classified information.

(4) *Timing for concurrence process.* (i) The CSA requests NID concurrence from the controlling agency as soon as the CSA has made a NID, if the entity needs access to SCI, RD, or COMSEC.

(ii) The controlling agency provides a final, written concurrence or non-concurrence to the CSA within 30 days after receiving the request for concurrence from the CSA.

(iii) In cases when a controlling agency requires clarification or additional information from the CSA, the controlling agency responds to the CSA within 30 days to request clarification or additional information as needed, and to coordinate a plan and timeline for concurring or non-concurring. The controlling agency must provide written updates to the CSA every 30 days until it concurs or non-concurs. In turn, the CSA provides the GCA and the entity with updates every 30 days.

(i) *Limited eligibility determinations (for entities under FOCI without mitigation or negation).* (1) In exceptional circumstances when an entity is under FOCI, the CSA may decide that limited eligibility for access to classified information is appropriate when the entity is unable or unwilling to implement FOCI mitigation or negation measures (this is not the same as limited eligibility in other circumstances; for more information on limited eligibility in other cases, see § 2004.32(f)).

(2) The GCA first decides whether to request a limited eligibility determination for the entity and must articulate a compelling need for it to the CSA that is in accordance with U.S. national security interests. The GCA must verify to the CSA that access to classified information is essential to contract or agreement performance, and accept the risk inherent in not mitigating or negating the FOCI. See § 2004.32(b)(3).

(3) The CSA may grant a limited eligibility determination if the GCA requests and the entity meets all other eligibility criteria in § 2004.32(e).

(4) A foreign government may sponsor a U.S. sub-entity of a foreign entity for limited eligibility when the foreign government desires to award a contract or agreement to the U.S. sub-entity that involves access to classified information for which the foreign government is the original classification authority (*i.e.*, foreign government information), and there is no other need for the U.S. sub-entity to have access to classified information.

(5) Limited eligibility determinations are specific to the classified information of the requesting GCA or foreign government, and specific to a single, narrowly defined contract, agreement, or circumstance of that GCA or foreign government.

(6) The access limitations of a favorable limited eligibility determination apply to all of the entity's employees, regardless of citizenship.

(7) A limited eligibility determination is not an option for entities that require access to proscribed information when a foreign government has ownership or control over the entity. See § 2004.32(e)(9).

(8) The CSA administratively terminates the entity's limited eligibility when there is no longer a need for access to the classified information for which the CSA made the favorable limited eligibility determination. Terminating one limited eligibility status does not impact other ones the entity may have.

§ 2004.36 Determining entity employee eligibility for access to classified information.

(a) *Making employee eligibility determinations.* (1) The responsible CSA:

(i) Determines whether entity employees meet the criteria established in the Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines (December 10, 2016). Entity employees must have a legitimate requirement (*i.e.*, need to know) for access to classified information in the performance of assigned duties and eligibility must be clearly consistent with the interest of the national security.

(ii) Notifies entities of its determinations of employee eligibility for access to classified information.

(iii) Terminates eligibility status when there is no longer a need for access to classified information by entity employees.

(2) The responsible CSA maintains:

(i) SF 312s, Classified Information Nondisclosure Agreements, or other approved nondisclosure agreements, executed by entity employees, as prescribed by ODNI in accordance with 32 CFR 2001.80 and E.O. 13526; and

(ii) Records of its entity employee eligibility determinations, suspensions, and revocations.

(3) CSAs ensure that entities limit the number of employees with access to classified information to the minimum number necessary to work on contracts or agreements requiring access to classified information.

(4) The CSA determines the need for event-driven reinvestigations for entity employees.

(5) CSAs use the Federal Investigative Standards (FIS) issued jointly by the Suitability and Security Executive Agents.

(6) The CSA provides guidance to entities on:

(i) Requesting employee eligibility determinations, to include guidance for submitting fingerprints; and

(ii) Granting employee access to classified information when the employee has had a break in access or a break in employment.

(7) If the CSA receives adverse information about an eligible entity employee, the CSA should consider and

possibly investigate, as authorized, to determine whether the employee's eligibility to access classified information remains clearly consistent with the interests of national security. If the CSA determines that an entity employee's continued eligibility is not in the interest of national security, the CSA implements procedures leading to suspension and ultimate revocation of the employee's eligible status, and notifies the entity.

(b) *Consultants.* A consultant is an individual under contract or agreement to provide professional or technical assistance to an entity in a capacity requiring access to classified information. A consultant is considered an entity employee for security purposes. The CSA makes eligibility determinations for entity consultants in the same way it does for entity employees.

(c) *Reciprocity.* The responsible CSA determines if an entity employee was previously investigated or determined eligible by another CSA. CSAs reciprocally accept existing employee eligibility determinations in accordance with applicable and current national level personnel security policy, and must not duplicate employee eligibility investigations conducted by another CSA.

(d) *Limited access authorization (LAA).* (1) CSAs may make LAA determinations for non-U.S. citizen entity employees in rare circumstances, when:

(i) A non-U.S. citizen employee possesses unique or unusual skill or expertise that the agency urgently needs to support a specific U.S. Government contract or agreement; and

(ii) A U.S. citizen with those skills is not available.

(2) A CSA may grant LAAs up to the secret classified level.

(3) CSAs may not use LAAs for access to:

(i) Top secret (TS) information;

(ii) RD or FRD information;

(iii) Information that a Government-designated disclosure authority has not determined releasable to the country of which the individual is a citizen;

(iv) COMSEC information;

(v) Intelligence information, to include SCI;

(vi) NATO information, except as follows: Foreign nationals of a NATO member nation may be authorized access to NATO information subject to the terms of the contract, if the responsible CSA obtains a NATO security clearance certificate from the individual's country of citizenship. NATO access is limited to performance on a specific NATO contract;

(vii) Information for which the U.S. Government has prohibited foreign disclosure in whole or in part; or

(viii) Information provided to the U.S. Government by another government that is classified or provided in confidence.

(4) The responsible CSA provides specific procedures to entities for requesting LAAs. The GCA must concur on an entity's LAA request before the CSA may grant it.

§ 2004.38 Safeguarding and marking.

(a) *Safeguarding approval.* (1) The CSA determines whether an entity's safeguarding capability meets requirements established in 32 CFR part 2001, and other applicable national level policy (*e.g.*, Atomic Energy Act for RD). If the CSA makes a favorable determination, the entity may store classified information at that level or below. If the determination is not favorable, the CSA must ensure that the entity does not possess classified information or does not possess information at the classification level denied or a higher level.

(2) The CSA maintains records of its safeguarding capability determinations and, upon request from GCAs or entities, and as appropriate and to the extent authorized by law, verifies that it has made a favorable safeguarding determination for a given entity and at what level.

(b) *Marking.* The GCA provides guidance to entities that meets requirements in 32 CFR 2001.22, 2001.23, 2001.24, and 2001.25, Derivative classification, Classification marking in the electronic environment, Additional requirements, and Declassification markings; ISOO's marking guide, *Marking Classified National Security Information;* and other applicable national level policy (*e.g.*, Atomic Energy Act for RD) for marking classified information and material.

§ 2004.40 Information system security.

(a) The responsible CSA must authorize an entity information system before the entity can use it to process classified information. The CSA must use the most complete, accurate, and trustworthy information to make a timely, credible, and risk-based decision whether to authorize an entity's system.

(b) The responsible CSA issues to entities guidance that establishes protection measures for entity information systems that process classified information. The responsible CSA must base the guidance on standards applicable to Federal systems, which must include the Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113–283, and may include National Institute of Standards and Technology (NIST) publications, Committee on National Security Systems (CNSS) publications, and Federal information processing standards (FIPS).

§ 2004.42 [Reserved]

APPENDIX A TO PART 2004—ACRONYM TABLE

For details on many of these terms, see the definitions at § 2004.4.

CCIPP—Classified Critical Infrastructure Protection Program
CCIPP POC—Entity point of contact under the CCIPP program
CIA—Central Intelligence Agency
CSA—Cognizant security agency
CNSS—Committee on National Security Systems
COMSEC—Communications security
CSO—Cognizant security office
DHS—Department of Homeland Security
DoD—Department of Defense
DOE—Department of Energy
EA—Executive agent (the NISP executive agent is DoD)
E.O.—Executive Order
FAR—Federal Aquisition Regulation
FOCI—Foreign ownership, control, or influence
GCA—Government contracting activity
Insider threat program SO—insider threat senior official (for an agency or for an entity)
ISOO—Information Security Oversight Office of the National Archives and Records Administration (NARA)
KMO—Key managers and officials (of an entity)
LAA—Limited access authorization
NID—National interest determination
NISPOM—National Industrial Security Program Operating Manual
NRC—Nuclear Regulatory Commission
NSA—National Security Agency
ODNI—Office of the Director of National Intelligence
PA—Proxy agreement
RD—Restricted data
SF—Standard Form
SAO—Senior agency official for NISP
SAP—Special access program
SCA—Security control agreement
SCI—Sensitive compartmented information
SSA—Special security agreement
TS—Top secret (classification level)
VT—Voting trust

PARTS 2005–2099 [RESERVED]