9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 7

Federal Emergency Management Agency

44 CFR Part 8

[DHS Docket No. DHS-2012-0067]

RIN 1601-AA68

Classified National Security Information

AGENCY: Office of the Secretary and Federal Emergency Management Agency, DHS.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security (DHS) is revising its procedures for managing classified national security information. DHS is updating its regulations to incorporate new and revised procedures pursuant to Executive Order 13526, "Classified National Security Information." Further, DHS is delegating to the Chief Security Officer of DHS the responsibility of serving as the "Senior Agency Official" pursuant to Executive Order 13526. The Chief Security Officer acted in this capacity under the predecessor Executive Order as well. Finally, DHS is also removing outdated regulations dealing with classified national security information at 44 CFR part 8.

DATES: This final rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: John Steele, Chief Policy Advisor, Office of the Chief Security Officer, Department of Homeland Security, (202) 447-0833

(not a toll-free number); Scott Ackiss, Chief, Administrative Security Division, Office of the Chief Security Officer, Department of Homeland Security, (202) 447-5341 (not a toll-free number).

SUPPLEMENTARY INFORMATION:

I. Background.

On December 29, 2009, the President issued Executive Order (E.O.) 13526, prescribing a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. 75 FR 707 (Jan. 5, 2010). E.O. 13526 replaced Executive Order 12958, 60 FR 19825 (Apr. 20, 1995), which had last been amended by E.O. 13292, 68 FR 15315 (Mar. 28, 2003).

DHS is amending its regulations to implement the revised requirements of E.O. 13526. The relevant changes relate to classification, safeguarding, and declassification of national security information. This rule is consistent with similar rules of other Executive Branch agencies relating to the classification, safeguarding, and declassification of classified national security information.

DHS is issuing this rule as a final rule without prior notice of proposed rulemaking because the procedures implemented under this final rule are largely mandated by Executive Order. Moreover, this rule, like similar rules of other Executive Branch agencies, is a rule of agency management, interpretation, or procedure. Such rules are exempt from prior notice and public comment under the Administrative Procedure Act (APA). 5 U.S.C. 553(a)(2), (b)(A). Consistent with its predecessor final rule implementing Executive Orders 12958 and 13292, see 70 FR 61211 (Oct. 21, 2005),

DHS has concluded that prior notice and opportunity for comment are therefore unnecessary. This rule is therefore effective upon publication.

E.O. 13526 requires that DHS make a number of technical changes to its regulations, including, for instance, removing references to outdated executive orders. In the interest of brevity, DHS is including in the discussion below only the most significant changes made in the regulations.

II. Analysis of this Final Rule.

This final rule establishes the procedures necessary for DHS to fulfill its obligations under E.O. 13526, "Classified National Security Information." This final rule does not address the Department's obligations under Executive Orders 13311, Homeland Security Information Sharing, 68 FR 45149 (July 31, 2003), or 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, 70 FR 62023 (Oct. 25, 2005), which deal with a related, but different, subject matter.

A. Subpart A – Administration.

Revised subpart A continues to delegate responsibility for administration of the DHS classification management program to the Chief Security Officer. Just as the Chief Security Officer acted in the capacity of "Senior Agency Official" under E.O. 12958, as amended, the Chief Security Officer will act as the Senior Agency Official under E.O. 13526. Similarly, subpart A continues to require components to designate a security officer/security liaison to implement and oversee the program at each component. Subpart A also sets forth potential administrative sanctions that may be imposed pursuant to E.O. 13526. See revised section 7.10(b)(11), 7.12(b). These provisions, which mirror provisions in the 2005 rule, are independent of criminal penalties that the Department of

Justice may prosecute. See, e.g., 18 U.S.C. 371, 792-798, 1001; 50 U.S.C. 783; 50 U.S.C. 421.

DHS is amending Subpart A to explicitly include in the delegation to the Chief Security Officer (1) responsibility for implementing and managing mandatory training for officials who hold original classification authority or perform derivative classification actions, and suspending classification authority of individuals who fail to attend such training, revised section 7.10(c)(3); (2) responsibility for reviewing and correcting classification decisions, revised section 7.10(c)(4); (3) authority to establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification, revised section 7.10(c)(10); (4) authority to establish and maintain a means to appoint, track, and train Department officials who do or will perform original and derivative classification actions, revised section 7.10(e); and (5) authority to implement, manage, and oversee a program providing access to and safeguarding classified information provided to non-federal entities, revised section 7.10(f).

DHS is also making technical amendments to other portions of sections 7.11 and 7.12, consistent with the Executive Order.

B. Subpart B – Classified Information.

Revised subpart B continues to provide DHS policy on the classification and declassification of national security information, including authority for the release of classified information to uncleared persons in an emergency. See, e.g., revised section 7.23. Subpart B also continues to provide the DHS processes for how to challenge the classification of information, including information classified by another agency, and how the public can submit a request for a mandatory review of classified information for

declassification and public release. See revised sections 7.31, 7.32.

Revised subpart B implements new standards for granting officials original classification authority, consistent with E.O. 13526. In revised section 7.20(a) and (b), DHS provides, consistent with section 1.3(c) of the Executive Order and predecessor executive orders, that neither the Secretary nor the Chief Security Officer may delegate original classification authority to any official who lacks a demonstrable and continuing need to exercise such authority.

Consistent with sections 1.3(d) and 2.1(d) of E.O. 13526, and as noted above in connection with the Chief Security Officer's authority under revised subpart A, revised subpart B implements new training requirements for original and derivative classifiers. Under revised section 7.20(c), DHS specifically requires officials delegated original classification authority to attend mandatory classification training within 60 days of the date of the delegation, and annually thereafter. Under revised section 7.26(d), those who perform derivative classification actions must attend mandatory derivative classification training before performing any derivative classification, and once every two years thereafter. The Chief Security Officer will suspend the classification authority of an official who does not complete the mandatory training, although the Chief Security Officer—or for cases involving the Inspector General, the Secretary or Deputy Secretary—may waive the suspension in exigent circumstances.

Changes under this subpart also implement the Executive Order's standards relating to whether and to what level DHS will classify information. In revised section 7.21(a)(4), DHS incorporates the explicit requirement in section 1.4 of E.O. 13526, which provides that information shall not be considered for classification unless, *inter alia*, its

unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security. Moreover, in revised section 7.21(c), DHS incorporates the new classification standards at section 1.1(b)-(c) of E.O. 13526. DHS clarifies, consistent with the Executive Order, that it will not classify information if there is significant doubt about the need to classify the information. If there is significant doubt about the appropriate level of classification, DHS will classify the information at the lower level. Finally, in revised section 7.21(e), DHS implements section 2.2(d)-(f) of the Executive Order, which requires agencies to incorporate original classification decisions into classification guides on a timely basis. DHS is requiring components to coordinate guides through the Chief Security Officer prior to approval and publication.

Changes to this subpart also implement new standards under which DHS will reclassify information. In revised section 7.21(g), the rule provides, consistent with section 1.7(c) of E.O. 13526, that information may not be reclassified after it has been declassified and released to the public under proper authority, unless, *inter alia*, the reclassification is approved in writing by the Secretary, based on a document-by-document determination that the reclassification of the information is required to prevent significant and demonstrable damage to the national security.

This rule also includes a number of new provisions relating to declassification. In revised section 7.20(e), DHS clarifies, consistent with section 3.1(b) of E.O. 13526, which officials may exercise declassification authority. Revised section 7.29 addresses DHS's role vis-à-vis the National Declassification Center, which the President established under section 3.7 of the Executive Order.

In new section 7.32 (which in many respects duplicates former section 7.31), consistent with section 3.5(g) of E.O. 13526, DHS now clarifies the mandatory declassification review process by defining who may request declassification review under the Executive Order. Proper requesters do not include foreign government entities or any representative thereof. New section 7.32 also clarifies that in general, DHS will deny requests for declassification review of overly broad categories of information, entire file series, and other similarly non-specific target information. Consistent with section 3.5(g) of E.O. 13526, new section 7.32 also now provides that mandatory declassification review does not apply to documents required to be submitted for prepublication review or other administrative process pursuant to an approved non-disclosure agreement. This would include, for instance, memoirs by current or former DHS employees, if a non-disclosure agreement applies.

DHS notes that the public's ability to request declassification of information under this rule is fully consistent with declassification provisions cited in EO 13526.

Finally, DHS is also making technical amendments to other portions of subpart B not referenced in this preamble, consistent with the Executive Order.

C. 44 CFR part 8

In this action, DHS is also removing outdated regulations dealing with the same subject matter at 44 CFR part 8.

III. Statutory and Regulatory Reviews.

A. Administrative Procedure Act.

DHS finds good cause to issue this rule without advance notice and public comment because such procedures are unnecessary. 5 U.S.C. 553(b)(B). As noted above, this

rulemaking incorporates into existing DHS regulations the provisions of E.O. 13526 without significant change. Further, this rule generally parallels the procedures currently used by other agencies to fulfill their obligations under Executive Order 13526.

Moreover, although this rulemaking includes certain delegations of authority not mandated by Executive Order 13526—such as, for instance, the delegation to the DHS Chief Security Officer in particular—such provisions plainly involve matters of internal DHS management and organization, i.e., DHS internal procedures for the classification and handling of classified national security information. See, e.g., 75 FR 37254 (June 28, 2010) (National Archives and Records Administration final rule); 76 FR 59031 (Sept. 23, 2011) (Central Intelligence Agency final rule). These provisions, as well as the remainder of the rule, are exempt from the APA's notice-and-comment requirements under 5 U.S.C. 553(a)(2).

For the same reasons, the Department has determined that this final rule should be issued without a delayed effective date pursuant to 5 U.S.C. 553(d)(3).

B. Regulatory Flexibility Act.

A Regulatory Flexibility Analysis is not required for this final rule because DHS is not required to publish a general notice of proposed rulemaking for this matter.

C. Executive Order 12866.

Executive Orders 13563 and 12866 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of

harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action" although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget. This rule incorporates into existing DHS regulations the requirements of Executive Order 13526 and also certain internal delegations of authority not mandated by Executive Order 13526. The rule's qualitative benefits include additional clarity for the public and DHS personnel with respect to Executive Order 13526's effect on DHS regulations. This rule imposes no additional costs on the public or the government.

D. Executive Order 12988.

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform.

E. Executive Order 13132.

This rule will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, DHS has determined that this rule does not have sufficient federalism implications to warrant the preparation of a federalism summary impact statement.

F. Unfunded Mandates Reform Act of 1995.

This rule will not result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions are

necessary under the provisions of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1501 et seq.

G. Small Business Regulatory Enforcement Fairness Act of 1996.

This rule is not a major rule as defined by section 251 of the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), 5 U.S.C. 804. This rule will not result in an annual effect on the economy of $100 million or more, a major increase in costs or prices, or significant adverse effects on competition, employment, investment, productivity, innovation, or the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

H. National Environmental Policy Act of 1969.

DHS has reviewed this action under Department of Homeland Security Management Directive 023-01, which guides the Department in complying with the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321 et seq.), and has concluded that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. Because this action involves administrative processing and document review functions, and because this action merely implements preexisting requirements, we have determined that it qualifies for, *inter alia*, categorical exclusions A1 and A3 of the Management Directive.

I. Paperwork Reduction Act

This rule does not contain any information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

J. Executive Order 13526.

This final rule has been reviewed by the Information Security Oversight Office of the National Archives and Records Administration pursuant to Executive Order 13526.

List of Subjects

6 CFR Part 7

Classified information, Organization, functions, and authority delegations.

44 CFR Part 8

Classified information

Accordingly, for the reasons set forth above, DHS amends 6 CFR chapter I, part 7, and 44 CFR chapter I, part 8, as follows:

Title 6 – Domestic Security

Chapter I – Department of Homeland Security, Office of the Secretary

1. In Chapter I, revise part 7 to read as follows:

PART 7 – CLASSIFIED NATIONAL SECURITY INFORMATION

Section

Subpart B – Classified Information

Authority: 5 U.S.C. 301; Pub. L. 107-296; E.O. 13526; 3 CFR, 1995 Comp., p. 333; E.O. 13142, 64 FR 66089, 3 CFR, 1999 Comp., p. 236; 32 CFR part 2001.

§ 7.1 Purpose.

The purpose of this part is to ensure that information within the Department of Homeland Security (DHS) relating to the national security is classified, safeguarded, and declassified pursuant to the provisions of Executive Order 13526, and implementing directives from the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA).

§ 7.2 Scope.

(a) This part applies to all employees, detailees, and non-contractor personnel inside and outside the Executive Branch who are granted access to classified information by the DHS, in accordance with the standards in Executive Order 13526, and its implementing directives, and Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and its implementing directives.

(b) This part does not apply to contractors, grantees and other categories of personnel falling under the purview of Executive Order 12829, National Industrial Security Program, as amended, and its implementing directives.

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions. This part does not, and is not intended to, create any right to judicial review of administrative action.

§ 7.3 Definitions.

The terms defined or used in Executive Order 13526, and the implementing directives in 32 CFR part 2001 and 2004 are applicable to this part.

Subpart A - Administration

§ 7.10 Authority of the DHS Chief Security Officer.

(a) The DHS Chief Security Officer (hereafter "Chief Security Officer") is designated as the Senior Agency Official as required by section 5.4(d) of Executive Order 13526, and, except as specifically provided elsewhere in this part, is authorized to administer the DHS Classified National Security Information program pursuant to Executive Order 13526.

(b) To the extent that 32 CFR part 2001 refers to the agency head or "designee," the Chief Security Officer is such designee unless determined otherwise by the Secretary. The Chief Security Officer may further delegate the associated authorities.

(c) The Chief Security Officer shall, among other actions:

(1) Oversee and administer the DHS's program established under Executive Order 13526;

(2) Promulgate implementing regulations;

(3) Establish and maintain DHS-wide security education and training programs, to include implementation and management of mandatory training for DHS officials who have been delegated original classification authority and those who perform derivative classification actions and suspension of such authority for failure to attend such training;

(4) Establish and maintain an ongoing self-inspection program that shall include regularly reviewing representative samples of DHS's original and derivative classification actions, correcting instances of misclassification, and reporting annually to the Director of ISOO on the DHS self-inspection program;

(5) Establish procedures to prevent unnecessary access to classified information, including procedures that:

(i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

(ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(6) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) Coordinate with the DHS Chief Human Capital Officer, as appropriate, to ensure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(i) Original classification authorities;

(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information, including persons who apply derivative classification markings;

(8) Account for the costs associated with implementing this part and report the cost to the Director of ISOO;

(9) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 13526, that pertains to classified information that originated in a DHS component that no longer exists and for which there is no clear successor in function;

(10) Establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification and to provide a ready source for guidance on proper classification;

(11) Report violations, take corrective measures and assess appropriate sanctions as warranted, in accordance with Executive Order 13526;

(12) Oversee DHS creation and participation in special access programs authorized under Executive Order 13526;

(13) Direct and administer DHS's personnel security program in accordance with Executive Order 12968 and other applicable law;

(14) Direct and administer DHS implementation and compliance with the National Industrial Security Program in accordance with Executive Order 12829 and other applicable guidance; and

(15) Perform any other duties as the Secretary may designate.

(d) The Chief Security Officer shall maintain a current list of all officials authorized pursuant to this part to originally classify or declassify documents.

(e) The Chief Security Officer shall establish and maintain a means for appointing, tracking, and training DHS officials who do or will perform original and derivative classification actions.

(f) The Chief Security Officer shall administer a program for the implementation, management, and oversight of access to and safeguarding of classified information provided to state, local, tribal, and private sector personnel pursuant to Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and its implementing directives.

(g) Nothing in this part will be interpreted to abrogate or affect the responsibilities of the Director of National Intelligence under the National Security Act of 1947, Pub. L. 235 (1947), as amended, and E.O. 12333, United States Intelligence Activities (1981), as

amended, or any responsibilities of the Under Secretary for Intelligence and Analysis conferred by presidential or intelligence community directive implicating those authorities, insofar as those authorities concern classified sources, methods, and activities, classified national intelligence, or sensitive compartmented information and are executed consistent with delegations or designations of authority issued pursuant to the statutory authority of the Secretary.

§ 7.11 Components' responsibilities.

Each DHS component shall appoint a security officer or security liaison to implement this part. The security officer/security liaison shall:

(a) Implement, observe, and enforce security regulations or procedures within their component with respect to the classification, declassification, safeguarding, handling, and storage of classified national security information;

(b) Report violations of the provisions of this part to the Chief Security Officer committed by employees of their component, as required by implementing directives;

(c) Ensure that employees of their component attend mandatory security education and training, as required by the DHS classified information security procedures, to include those component officials delegated the authority to classify information originally and those who perform derivative classification actions;

(d) Continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or reduce the level of access authorized, as appropriate; and

(e) Cooperate fully with any request from the Chief Security Officer for assistance in the implementation of this part.

§ 7.12 Violations of classified information requirements.

(a) Any person who suspects or has knowledge of a violation of this part, including the known or suspected loss or compromise of classified information, shall promptly report such violations or possible violations, pursuant to requirements set forth in DHS directives.

(b) DHS employees and detailees may be reprimanded, suspended without pay, terminated from classification authority, suspended from or denied access to classified information, or subject to other sanctions in accordance with applicable law and DHS regulations or directives if they:

(1) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under Executive Order 13526, or its predecessor orders;

(2) Knowingly, willfully, or negligently classify or continue the classification of information in violation of Executive Order 13526, or its implementing directives; or

(3) Knowingly, willfully, or negligently create or continue a special access program contrary to the requirements of Executive Order 13526; or,

(4) Knowingly, willfully, or negligently violate any other provision of Executive Order 13526, or DHS implementing directives, or;

(5) Knowingly, willfully, or negligently grant eligibility for, or allow access to, classified information in violation of Executive Order 13526, or its implementing directives, this part, or DHS implementing directives promulgated by the Chief Security Officer.

§ 7.13 Judicial proceedings.

(a) Any DHS official or organization, except for the Office of Inspector General in matters involving the Office of Inspector General only, receiving an order or subpoena from a federal or state court, or an administrative subpoena from a federal agency, to produce classified information (see 6 CFR 5.41 through 5.49), required to submit classified information for official DHS litigation purposes, or receiving classified information from another organization for production of such in litigation, shall notify the Office of the General Counsel, unless the demand for production is made by the Office of the General Counsel, and immediately determine from the agency originating the classified information whether the information can be declassified. If declassification is not possible, DHS representatives will take appropriate action to protect such information, pursuant to the provisions of this section.

(b) If a determination is made under paragraph (a) of this section to produce classified information in a judicial proceeding in any manner, the DHS General Counsel attorney, or the Office of Inspector General attorney, if the matter involves the Office of Inspector General only, in conjunction with the Department of Justice, shall take appropriate steps to protect classified information in judicial proceedings and retrieve the information when the information is no longer required in such judicial proceedings, in accordance with the Department of Justice procedures, and in Federal criminal cases, pursuant to the requirements of Classified Information Procedures Act (CIPA), Pub. L. 96-456, 94 Stat. 2025, (18 U.S.C. App.), and the "Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information," and other applicable authorities.

Subpart B – Classified Information

§ 7.20 Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Secretary and by officials with a demonstrable and continuing need to exercise such authority and to whom such authority is delegated in writing by the Secretary. The Chief Security Officer, as the Senior Agency Official, is delegated authority to originally classify information up to and including Top Secret. No official who is delegated Top Secret original classification authority by the Secretary may further delegate such authority.

(b) The Chief Security Officer may delegate Secret and Confidential original classification authority to other officials with a demonstrable and continuing need to exercise such authority. No official who is delegated original classification authority by the Secretary or the Chief Security Officer may further delegate such authority.

(c) Persons who are delegated original classification authority shall attend mandatory classification training within 60 days of the delegation, and annually thereafter. Persons who fail to attend mandatory training shall have such authority suspended until such time as the training occurs.

(1) Except for suspensions of the Inspector General's classification authority, the Chief Security Officer may waive a suspension of authority for no longer than 60 days following the due date of the training when unavoidable circumstances exist that prevent the person from attending the training.

(2) For cases involving suspension of the Inspector General's classification authority under paragraph (c) of this section, only the Secretary or Deputy Secretary may waive such a suspension.

(d) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level. In the absence of an official authorized to exercise classification authority, the person designated to act in lieu of such official may exercise the official's classification authority.

(e) Declassification authority may be exercised by the official who authorized the original classification, if that official is still serving in the same position and has original classification authority; the originator's current successor in function, if that individual has original classification authority; a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or officials delegated declassification authority by the Secretary or the Chief Security Officer.

§ 7.21 Classification of information, limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) An original classification authority is classifying the information;

(2) The information is owned by, produced by or for, or is under the control of the United States Government;

(3) The information falls within one or more of the categories of information specified in section 1.4 of Executive Order 13526; and

(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to cause identifiable and describable damage to the national security.

(b) Information shall be classified as Top Secret, Secret, or Confidential in accordance with and in compliance with the standards and criteria in Executive Order 13526. No other terms shall be used to identify United States classified information except as otherwise provided by statute.

(c) If there is significant doubt about the need to classify information it shall not be classified. If classification is warranted but there is significant doubt about the appropriate level of classification it shall be classified at the lower level.

(d) Original classification decisions made by a DHS original classification authority shall be incorporated into a security classification guide in a timely manner but no later than one year from the date of the original decision. Such decisions shall be reported to the Office of the Chief Security Officer, Administrative Security Division, within thirty days following the original classification decision.

(e) All DHS security classification guides shall be coordinated through and receive the concurrence of the Office of the Chief Security Officer, Administrative Security Division, prior to approval and publication by an original classification authority.

(f) Information shall not be classified in order to:

(1) Conceal inefficiency, violations of law, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition;

(4) Prevent or delay release of information that does not require protection in the interest of national security.

(g) Information may not be reclassified after it has been declassified and released to the public under proper authority unless:

(1) The reclassification is approved in writing by the Secretary based on a document-by-document determination that the reclassification of the information is required to prevent significant and demonstrable damage to the national security;

(2) The reclassification of the information meets the standards and criteria for classification pursuant to Executive Order 13526;

(3) The information may be reasonably recovered without bringing undue attention to the information; and

(4) The reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of ISOO.

(5) For documents in the physical and legal custody of the National Archives and Records Administration that have previously been made available for public use and determined to warrant reclassification per paragraphs (g)(1) through (4) of this section, the Secretary shall notify the Archivist of the United States, who shall suspend public access pending approval by the Director of ISOO. Any such decision made by the Director of ISOO may be appealed by the Secretary to the President through the National Security Advisor.

(h) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after DHS has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 13526, section 3.5. When it is necessary to classify or reclassify such information, it shall be done so on a document-by-document basis with the personal participation of and under the direction of the Secretary or Deputy Secretary.

§ 7.22 Classification pending review.

(a) Whenever persons who do not have original classification authority originate or develop information that they believe requires immediate classification and safeguarding, and no authorized original classifier is available, that person shall:

(1) Safeguard the information in a manner appropriate for the classification level they believe it to be;

(2) Apply the appropriate overall classification markings; and

(3) Within five working days, securely transmit the information to the organization that has appropriate subject matter interest and original classification authority.

(b) When it is not clear which component would be the appropriate original classifier, the information shall be sent to the Office of the Chief Security Officer, Administrative Security Division, to determine the appropriate organization.

(c) The applicable original classification authority shall decide within 30 days of receipt whether the information warrants classification pursuant to Executive Order 13526 and shall render such decision in writing.

§ 7.23 Emergency release of classified information.

(a) The DHS Undersecretary for Management has delegated to certain DHS employees the authority to disclose classified information to an individual or individuals not otherwise eligible for access in emergency situations when there is an imminent threat to life or in defense of the homeland.

(b) In exercising this authority, the delegees shall adhere to the following conditions:

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

(2) Limit the number of individuals who receive it to only those persons with a specific need-to-know;

(3) Transmit the classified information through approved communication channels by the most secure and expeditious method possible, or by other means deemed necessary in exigent circumstances;

(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 as determined by the delegated official;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain from the recipients a signed DHS Emergency Release of Classified Information Non-disclosure Form. In emergency situations requiring immediate verbal release of information, the signed nondisclosure agreement memorializing the briefing may be received after the emergency abates;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 7 days after the release, the disclosing authority must notify the DHS Office of the Chief Security Officer, Administrative Security Division, and the originating agency of the information disclosed. A copy of the signed nondisclosure agreements should be forwarded with the notification, or as soon thereafter as practical.

(7) Release of information pursuant to this authority does not constitute declassification of the information.

(8) Authority to disclose classified information under the above conditions may not be further delegated.

§ 7.24 Duration of classification.

(a) At the time of original classification, original classification authorities shall apply a date or event in which the information will be automatically declassified.

(b) The original classification authority shall attempt to establish a specific date or event that is not more than 10 years from the date of origination in which the information will be automatically declassified. If the original classification authority cannot determine an earlier specific date or event it shall be marked for automatic declassification 10 years from the date of origination.

(c) If the original classification authority determines that the sensitivity of the information requires classification beyond 10 years, it may be marked for automatic declassification for up to 25 years from the date of the original classification decision.

(d) Original classification authorities do not have the authority to classify or retain the classification of information beyond 25 years from the date of origination. The only exceptions to this rule are information that would clearly and demonstrably be expected to reveal the identity of a confidential human source or human intelligence source, or, key design concepts of weapons of mass destruction. In these instances, the information shall be marked for declassification based on implementing directives issued pursuant to Executive Order 13526. In all other instances, classification beyond 25 years shall only be authorized in accordance with § 7.28 and Executive Order 13526.

§ 7.25 Identification and markings.

(a) Classified information, in all forms, must be marked in a manner that is immediately apparent pursuant to the standards set forth in section 1.6 of Executive Order 13526; 32 CFR part 2001, subpart B; and internal DHS guidance approved and distributed by the Office of the Chief Security Officer.

(b) Foreign government information shall retain its original classification markings or be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(c) Information assigned a level of classification under predecessor Executive Orders shall remain classified at that level of classification, except as otherwise provided herein, i.e., the information is reclassified or declassified.

§ 7.26 Derivative classification.

(a) Derivative classification is defined as the incorporating, paraphrasing, restating, or generating in a new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Information is also derivatively classified when classification is based on instructions provided in a security classification guide.

(b) Persons need not possess original classification authority to derivatively classify information based on source documents or classification guides.

(c) Persons who perform derivative classification actions shall be designated as authorized derivative classifiers as specified in directives published by the Office of the Chief Security Officer.

(d) Persons who are designated as authorized derivative classifiers shall attend mandatory classification training before performing derivative classification actions, and

once every two years thereafter. Persons who fail to attend mandatory training shall have such authority suspended until such time as the training occurs.

(1) Except for suspensions of the Office of Inspector General's classification authority, the Chief Security Officer may waive the suspension of authority for no longer than 60 days following the due date of the training when unavoidable circumstances exist that prevent the person from attending the training.

(2) For cases involving suspension of the Office of Inspector General's classification authority under paragraph (d) of this section, only the Secretary or Deputy Secretary may waive such a suspension.

(e) Persons who apply derivative classification markings shall observe original classification decisions and carry forward to any newly created documents the pertinent classification markings.

(f) Information classified derivatively from other classified information shall be classified and marked in accordance with the standards set forth in sections 2.1 and 2.2 of Executive Order 13526, 32 CFR part 2001, and internal DHS guidance provided by the Office of the Chief Security Officer.

§ 7.27 Declassification and downgrading.

(a) Classified information shall be declassified as soon as it no longer meets the standards for classification. Declassification and downgrading is governed by part 3 of Executive Order 13526, implementing ISOO directives at 32 CFR part 2001, subpart C, and applicable internal DHS direction provided by the Office of the Chief Security Officer.

(b) Information shall be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position and has original classification authority, the originator's successor if that position has original classification authority, or a supervisory official of either if that position has original classification authority, or, by officials delegated such authority in writing by the Secretary or the Chief Security Officer, or, pursuant to section 3.1.(e) of Executive Order 13526, the Director of the Information Security Oversight Office.

(c) It is presumed that information that continues to meet the classification requirements under Executive Order 13526 requires continued protection. In some exceptional cases during declassification reviews, the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. If it appears that the public interest in disclosure of the information may outweigh the need to protect the information, the declassification reviewing official shall refer the information with a recommendation for decision to the Chief Security Officer. The Chief Security Officer shall review the information and after consulting with the applicable original classification authority and other components and agencies with equities, make a recommendation to the Secretary on whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. The Secretary shall decide whether to declassify the information. The decision of the Secretary shall be final. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.

(d) Each component shall develop schedules for declassification of records in the National Archives.

§ 7.28 Automatic declassification.

(a) Subject to paragraph (b) of this section and paragraphs 3.3(b) - (d) and (g) - (j) of Executive Order 13526, all classified information contained in records that are more than 25 years old that have been determined to have permanent historical value shall be declassified automatically on December 31st of the year that is 25 years from the date of origin.

(b) At least one year before information is declassified automatically under this section, the Chief Security Officer shall notify the ISOO of any specific information that DHS proposes to exempt from automatic declassification. The notification shall include:

(1) A description of the information;

(2) An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) A specific date or event for declassification of the information whenever the information exempted does not identify a confidential human source or human intelligence source, or, key design concepts of weapons of mass destruction.

(c) Proposed exemptions under this section shall be forwarded to the Chief Security Officer. When the Chief Security Officer determines the exemption request is consistent with this section, he or she will submit the exemption request to the Executive Secretary of the Interagency Security Classification Appeals Panel (ISCAP) for approval.

(d) Declassification guides that narrowly and precisely define exempted information may be used to exempt information from automatic declassification. Declassification

guides must include the exemption notification information detailed in paragraph (b) of this section, and be approved pursuant to paragraph (c) of this section. The creation of declassification guides to cite proposed or ISCAP-approved DHS exemptions shall be coordinated through and processed by the Office of the Chief Security Officer, Administrative Security Division.

§ 7.29 National Declassification Center.

(a) The Chief Security Officer and applicable components will support the NARA, National Declassification Center (NDC), which was established to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. The Chief Security Officer will assign DHS personnel on an as-needed basis to address declassification matters and priorities containing DHS equities.

(b) The Office of the Chief Security Officer shall provide the NDC with all DHS classification and declassification guides that include ISCAP-approved exemptions from automatic declassification.

(c) The Chief Security Officer, or his designee, shall oversee DHS-wide support to the NDC, including representing DHS in consultations with the NDC Director.

§ 7.30 Documents of permanent historical value.

The original classification authority, to the greatest extent possible, shall declassify classified information contained in records determined to have permanent historical value under 44 U.S.C. 2107 before they are accessioned into the National Archives.

§ 7.31 Classification challenges.

(a) Authorized holders of information classified by DHS or any other agency who, in good faith, believe that specific information is improperly or unnecessarily classified are encouraged and expected to challenge the classification status of that information pursuant to section 1.8 of Executive Order 13526. Authorized holders may submit classification challenges in writing to the original classification authority with jurisdiction over the information in question. If an original classification authority cannot be determined, the challenge shall be submitted to the Office of the Chief Security Officer, Administrative Security Division. The challenge need not be more specific than a question as to why the information is or is not classified, or is classified at a certain level.

(b) If anonymity of the challenger is requested, the challenger may submit the challenge to the Office of the Chief Security Officer, Administrative Security Division. The Administrative Security Division will act as an agent for the challenger and the identity of the challenger will be redacted.

(c) The original classification authority shall no later than 60 days from receipt of the challenge, provide a written response to the submitter. The original classification authority may classify or declassify the information subject to the challenge and, if applicable, state specific reasons why the original classification determination was proper. If the original classification authority is not able to respond within 60 days, he or she shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(d) The individual challenging the classification will be notified of the determination made by the original classification authority and that the individual may appeal this determination to the Chief Security Officer, or in cases involving appeals by Office of

Inspector General employees, the Secretary or Deputy Secretary. Upon receipt of such appeals, the Chief Security Officer, or in cases involving appeals by Office of Inspector General employees, the Secretary or Deputy Secretary, shall convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP shall, at a minimum, consist of representatives from the Office of the Chief Security Officer, the Office of General Counsel, and a representative from the component having jurisdiction over the information. Additional members may be added as determined by the Chief Security Officer. The DHS/CAP shall be chaired by the Chief Security Officer.

(e) If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel (ISCAP) pursuant to section 5.3 of Executive Order 13526, and the rules issued by the ISCAP pursuant to section 5.3 of Executive Order 13526.

(f) Any individual who challenges a classification and believes that any action has been taken against him or her in retaliation or retribution because of that challenge may report the facts to the Office of Inspector General via its Hotline or website, or other appropriate office.

(g) Nothing in this section shall prohibit a person from informally challenging the classified status of information directly to the original classification authority.

(h) Classification challenge provisions are not applicable to documents required to be submitted for prepublication review or other administrative process pursuant to an approved non-disclosure agreement.

(i) Requests for review of classified material for declassification by persons other than authorized holders are governed by § 7.32.

§ 7.32 Mandatory declassification review.

(a) Any individual, as "individual" is defined by 5 U.S.C. 552a(a)(2) (with the exception of a foreign government entity or any representative thereof), may request that classified information be reviewed for declassification pursuant to the mandatory declassification review provisions of section 3.5 of Executive Order 13526. Such requests must be sent to the Departmental Disclosure Officer, Privacy Office, 245 Murray Lane, S.W., Building 410, Washington, D.C. 20528.

(b) The request must describe the document or material with enough specificity to allow it to be located by the component with a reasonable amount of effort. Components will generally consider deficient any requests for declassification review of, for instance, broad categories of information, entire file series of records, or similar non-specific requests.

(1) When the description of the information in the request is deficient, the component shall solicit as much additional identifying information as possible from the requester.

(2) If the information or material requested cannot be obtained with a reasonable amount of effort, the component shall provide the requester, through the DHS Disclosure Officer, with written notification of the reasons why no action will be taken and of the requester's right to appeal.

(c) Requests for review of information that has been subjected to a declassification review request within the preceding two years shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.

(d) Mandatory Declassification Review provisions are not applicable to documents required to be submitted for prepublication review or other administrative process pursuant to an approved non-disclosure agreement.

(e) Requests for information exempted from search or review under sections 701, 702, or 703 of the National Security Act of 1947, as added and amended (50 U.S.C. 431 – 433), or other provisions of law, shall not be processed. The DHS Disclosure Officer will notify the requester of such denial.

(f) If documents or material being reviewed for declassification under this section contain information that has been originally classified by another government agency, the reviewing authority shall notify the DHS Disclosure Officer. Unless the association of that organization with the requested information is itself classified, the DHS Disclosure Officer will then notify the requester of the referral.

(g) A DHS component may refuse to confirm or deny the existence, or non-existence, of requested information when its existence or non-existence, is properly classified.

(h) DHS components shall make a final determination on the request as soon as practicable but within one year from receipt. When information cannot be declassified in its entirety, components shall make reasonable efforts to redact those portions that still meet the standards for classification and release those declassified portions of the requested information that constitute a coherent segment.

(i) DHS components shall notify the DHS Disclosure Officer of the determination made in the processing of a mandatory review request. Such notification shall include

the number of pages declassified in full; the number of pages declassified in part; and the number of pages where declassification was denied.

(j) The DHS Disclosure Officer shall maintain a record of all mandatory review actions for reporting in accordance with applicable Federal requirements.

(k) The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal the denial of declassification. To address such appeals, the DHS Disclosure Office shall convene a DHS Classification Appeals Panel (DHS/CAP). The DHS/CAP shall, at a minimum, consist of representatives from the Disclosure Office, the Office of the Chief Security Officer, the Office of General Counsel, and a representative from the component having jurisdiction over the information. Additional members may be added as determined by the DHS Disclosure Officer. The DHS/CAP shall be chaired by the DHS Disclosure Officer.

(l) If the requester files an appeal through the DHS/CAP, and the appeal is denied, the requester shall be notified of the right to appeal the denial to the ISCAP pursuant to section 5.3 of Executive Order 13526, and the rules issued by the ISCAP pursuant to section 5.3 of Executive Order 13526.

Title 44 – Emergency Management and Assistance

Chapter I – Federal Emergency Management Agency, Department of Homeland Security

Part 8—[Removed and reserved]

2. Under the authority of 5 U.S.C. 301 and E.O. 13526, remove and reserve part 8, consisting of §§ 8.1 through 8.4.

_____

Jeh Charles Johnson,
Secretary.

[FR Doc. 2014-17836 Filed 07/29/2014 at 8:45 am; Publication Date: 07/30/2014]