

## § 7.22

## 6 CFR Ch. I (1–1–07 Edition)

(3) The information may be reasonably recovered; and

(4) The reclassification action is reported promptly to the Director of ISOO.

(e) 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 Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 12958, as amended, section 3.5. When it is necessary to classify or reclassify such information, it shall be forwarded to the Chief Security Officer and classified or reclassified only at the direction of the Secretary or Deputy Secretary of Homeland Security.

### § 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 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 classification authority.

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

(c) The organization with classification authority shall decide within 30 days whether to classify the information.

### § 7.23 Emergency release of classified information.

(a) The Secretary of Homeland Security has delegated to certain DHS employees the authority to disclose classified information to an individual or individuals not otherwise routinely eligible for access in emergency situa-

tions when there is an imminent threat to life or in defense of the homeland.

(b) In exercising this authority, the delegates 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 Chief Security Officer and the originating agency of the information disclosed. A copy of the signed nondisclosure agreements should be forwarded with the notification under this paragraph (b)(6), 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 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 not more than 10 years after 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 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 exception to this rule is when disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. In this instance, the information may be marked for declassification as "25X1-Human," indicating that the information is exempt from the "25 Year Rule" for automatic declassification. This marking is not authorized for use when the information pertains to non-human intelligence sources or intelligence methods. In all other instances, classification beyond 25 years shall only be authorized in accordance with § 7.28 of this part and Executive Order 12958, as amended.

#### § 7.25 Identification and markings.

(a) Classified information must be marked pursuant to the standards set forth in section 1.6 of Executive Order 12958, as amended; 32 CFR part 2001, subpart B; and internal DHS guidance provided by 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 Execu-

tive 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 apply derivative classification markings shall observe original classification decisions and carry forward to any newly created documents the pertinent classification markings.

(d) 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 12958, as amended, 32 CFR 2001.22, and internal DHS guidance provided by 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 12958, as amended, implementing ISOO directives at 32 CFR part 2001, subpart C, and applicable internal DHS direction provided by 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, the originator's successor, or a supervisory official of either, or by officials delegated such authority in writing by the Secretary of Homeland Security or the Chief Security Officer.