

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 pub-

lic 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.