

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.