

(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

§ 2001.53

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 sound baffles, or an intrusion detection system.

(d) *Windows.* (1) All windows which might reasonably afford visual observa-

32 CFR Ch. XX (7-1-10 Edition)

tion 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