

§ 2001.41

Security Authority for NATO Instructions I-69 and I-70. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation). When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at §2001.53 may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) An agency head who originates or handles classified information shall refer any matter pertaining to the implementation of this Directive that he or she cannot resolve to the Director, ISOO for resolution.

§ 2001.41 Responsibilities of holders [4.1].

Authorized persons who have access to classified information are responsible for:

(a) Protecting it from persons without authorized access to that information, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person;

(b) Meeting safeguarding requirements prescribed by the agency head; and

(c) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

§ 2001.42 Standards for security equipment [4.1].

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment

32 CFR Ch. XX (7-1-04 Edition)

is procured, it shall be in conformance with the standards and specifications established by the Administrator of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

§ 2001.43 Storage [4.1].

(a) *General.* Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) *Requirements for physical protection.* (1) Top Secret. Top Secret information shall be stored by one of the following methods:

(i) In a GSA-approved security container with one of the following supplemental controls:

(A) Continuous protection by cleared guard or duty personnel;

(B) Inspection of the security container every two hours by cleared guard or duty personnel;

(C) An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation [Acceptability of Intrusion Detection Equipment (IDE): All IDE must be UL-listed (or equivalent as defined by the agency head) and approved by the agency head. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head.]; or

(D) Security-In-Depth conditions, provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.

(ii) An open storage area constructed in accordance with §2001.43, which is equipped with an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not.

(iii) An IDS-equipped vault with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) Secret. Secret information shall be stored by one of the following methods:

(i) In the same manner as prescribed for Top Secret information;

(ii) In a GSA-approved security container or vault without supplemental controls; or

(iii) In either of the following:

(A) Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock; or

(B) An open storage area. In either case, one of the following supplemental controls is required:

(1) The location that houses the container or open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(2) Cleared guard or duty personnel shall inspect the security container or open storage area once every four hours; or

(3) An IDS (per paragraph (b)(1)(i)(C) of this section) with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation. [In addition to one of these supplemental controls specified in paragraphs (b)(2)(iii)(B)(1) through (3), security-in-depth as determined by the agency head is required as part of the supplemental controls for a non-GSA-approved container or open storage area storing Secret information.]

(3) Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

(c) *Combinations.* Use and maintenance of dial-type locks and other changeable combination locks.

(1) Equipment in service. The classification of the combination shall be the same as the highest level of classified information that is protected by the lock. Combinations to dial-type locks shall be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the

level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(i) Whenever such equipment is placed into use;

(ii) Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(iii) Whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the built-in combination lock shall be reset to a standard combination.

(d) *Key operated locks.* When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established.

§ 2001.44 Information controls [4.1, 4.2].

(a) *General.* Agency heads shall establish a system of control measures which assure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(b) *Reproduction.* Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken: