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 Appendix B 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.

§ 2004.3 Definitions.

(a) Open storage area. An area, constructed in accordance with Appendix A and authorized by the agency head for open storage of classified information.

(b) Authorized person. A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

(c) Cleared commercial carrier. A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

(d) Security-in-depth. A determination by the agency head that a facility’s security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during non-working hours.

(e) Vault. An area approved by the agency head which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry. A modular vault approved by the General Services Administration (GSA) may be used in lieu of a vault as prescribed in the first sentence of this paragraph (e). Vaults shall be equipped with a GSA-approved vault door and lock.

§ 2004.4 Responsibilities of holders.

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.

§ 2004.5 Standards for security equipment.

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 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.