§ 2003.32 DATA DESCRIPTOR Label SF 711.

(a) SF 711 is used to identify additional safeguarding controls that pertain to classified information that is stored or contained on automatic data processing (ADP) or other media.

(b) SF 711 shall be used in all situations that require the use of a DATA DESCRIPTOR Label. Agency-wide use of SF 711 shall begin when supplies of existing forms are exhausted or January 31, 1988, whichever occurs earlier.

(c) SF 711 is affixed to the ADP medium containing classified information in a manner that would not adversely affect operation of equipment in which the medium is used. SF 711 is ordinarily used in conjunction with the SF 706, SF 707, SF 708 or SF 709, as appropriate. Once the Label has been applied, it cannot be removed. The SF 711 provides spaces for information that should be completed as required.

(d) Only the Director of ISOO may grant a waiver from the use of SF 711. To apply for a waiver, an agency must submit its proposed alternative form to the Director of ISOO along with its justification for use. The Director of ISOO will review the request and notify the agency of the decision.

(e) The national stock number of the SF 711 is 7540–01–207–5541.

[52 FR 10191, Mar. 30, 1987]

PART 2004—DIRECTIVE ON SAFE-GUARDING CLASSIFIED NATIONAL SECURITY INFORMATION

Sec.
2004.1 Authority.
2004.2 General.
2004.3 Definitions.
2004.4 Responsibilities of holders.
2004.5 Standards for security equipment.
2004.6 Storage.
2004.7 Information controls.
2004.8 Transmission.
2004.9 Destruction.
2004.10 Loss, possible compromise or unauthorized disclosure.
2004.11 Special access programs.
2004.12 Telecommunications, automated information systems and network security.

APPENDIX B TO PART 2004—FOREIGN GOVERNMENT INFORMATION

SOURCE: 64 FR 51854, Sept. 24, 1999, unless otherwise noted.

§ 2004.1 Authority.

This Directive is issued pursuant to Section 5.2 (c) of Executive Order (E.O.) 12958, “Classified National Security Information.” The E.O. and this Directive set forth the requirements for the safeguarding of classified national security information (hereinafter classified information) and are applicable to all U.S. Government agencies.

§ 2004.2 General.

(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for NATO and other foreign government information, agency heads or their designee(s) (hereinafter referred to as agency heads) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director, Information Security Oversight Office (ISOO), to facilitate that office’s oversight responsibility. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasures benefits versus cost.

(c) NATO classified information shall be safeguarded in compliance with U.S.
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 through-out 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 Administration of General Services, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.