§ 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 NA-
TIONAL 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 A TO PART 2004—OPEN STORAGE AREAS.

APPENDIX B TO PART 2004—FOREIGN GOVERN-
MENT 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.