

Director of ISOO for guidance and assistance. The Director of ISOO, in consultation with other agencies, as appropriate, will ensure that the safeguarding and declassification requirements of the Order are met.

**§ 2001.37 Assistance to the Department of State.**

Heads of agencies shall assist the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by facilitating access to appropriate classified materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS. If an agency fails to provide a final declassification review determination regarding a Department of State referral within 120 days of the date of the referral, or if applicable, within 120 days of the date of a High Level Panel decision, the Department of State, consistent with 22 U.S.C. 4353 and any implementing agency procedures, may seek the assistance of the Panel.

**Subpart E—Safeguarding**

**§ 2001.40 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 foreign government information, agency heads or their designee(s) 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 of ISOO. 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 antici-

pated threats; vulnerability; and countermeasure benefits versus cost.

(c) North Atlantic Treaty Organization (NATO) classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instruction (USSAN) 1-07. 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 § 2001.54 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) *Need-to-know determinations.* (1) Agency heads, through their designees, shall identify organizational missions and personnel requiring access to classified information to perform or assist in authorized governmental functions. These mission and personnel requirements are determined by the functions of an agency or the roles and responsibilities of personnel in the course of their official duties. Personnel determinations shall be consistent with section 4.1(a) of the Order.

(2) In instances where the provisions of section 4.1(a) of the Order are met, but there is a countervailing need to restrict the information, disagreements that cannot be resolved shall be referred by agency heads or designees to either the Director of ISOO or, with respect to the Intelligence Community, the Director of National Intelligence, as appropriate. Disagreements concerning information protected under section 4.3 of the Order shall instead be referred to the appropriate official named in section 4.3 of the Order.

**§ 2001.41 Responsibilities of holders.**

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