Formerly Restricted Data shall be referred to the Department of Energy through the NDC. If the Department of Energy confirms that the document contains Restricted Data or Formerly Restricted Data, it shall then be excluded from the automatic declassification provisions of the Order until the Restricted Data or Formerly Restricted Data designation is properly removed.

(i) When the Department of Energy provides notification that a Restricted Data or Formerly Restricted Data designation is not appropriate or when it is properly removed, the record shall be processed for automatic declassification through the NDC.

(ii) In all cases, should the record be the subject of an access demand made pursuant to the Order or provision of law, the information classified pursuant to Executive order (rather than the Atomic Energy Act, as amended) must stand on its own merits.

(9) The NDC, as well as any centralized agency facility established under section 3.7(e) of the Order, shall track and document referral actions and decisions in a manner that facilitates archival processing for public access. Central agency facilities must work with the NDC to ensure documentation meets NDC requirements, and transfer all documentation on pending referral actions and referral decisions to the NDC when transferring the records to NARA.

(10) In all cases, receiving agencies shall acknowledge receipt of formal referral notifications in a timely manner. If a disagreement arises concerning referral notifications, the Director of ISOO will determine the automatic declassification date and notify the senior agency official, as well as the NDC or the primary reviewing agency.

(11) *Remote Archives Capture (RAC).* Presidential records or materials scanned in the RAC process shall be prioritized and scheduled for review by the NDC. The initial notification shall be made to the agency with primary equity, which shall have up to one year to act on its information and to identify all other equities eligible for referral. All such additional referrals in an individual record shall be made at the same time, and once notified by the NDC of an eligible referral, such receiving agencies shall have up to one year to review the records before the onset of automatic declassification.

(c) *Agencies eligible to receive referrals.* The Director of ISOO will publish annually a list of those agencies eligible to receive referrals for each calendar year.

(d) *Systematic declassification review.* The identification of equities shall be accomplished in accordance with paragraph (b) of this section. Priorities for review will be established by the NDC.

(e) *Identification of interests other than national security.* Referrals under sections 3.3(d)(3) and 3.6(b) of the Order shall be assumed to be intended for later public release unless withholding is otherwise authorized and warranted under applicable law. If a receiving agency proposes to withhold any such information, it must notify the referring agency at the time they otherwise respond to the referral. Such notification shall identify the specific information at issue and the pertinent law.

### § 2001.35 Discretionary declassification.

(a) In accordance with section 3.1(d) of the Order, agencies may declassify information when the public interest in disclosure outweighs the need for continued classification.

(b) Agencies may also establish a discretionary declassification program that is separate from their automatic, systematic, and mandatory review programs.

### § 2001.36 Classified information in the custody of private organizations or individuals.

(a) *Authorized holders.* Agencies may allow for the holding of classified information by a private organization or individual provided that all access and safeguarding requirements of the Order have been met. Agencies must provide declassification assistance to such organizations or individuals.

(b) *Others.* Anyone who becomes aware of organizations or individuals who possess potentially classified national security information outside of government control must contact the

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 anticipated 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: