12958, by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) *Significant interagency support requirements.* Agency heads must ensure that a Memorandum of Agreement/Understanding (MOA/MOU) is established for each Special Access Program that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

§ 2004.12 Telecommunications, automated information systems and network security.

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Index of National Security Telecommunications and Information Systems Security Issuances (NSTISSI) and Director of Central Intelligence Directive (DCID) 6/3.

§ 2004.13 Technical security.

Based upon the risk management factors referenced in § 2004.2 of this directive agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures (TSCM) and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, entitled Tempest Countermeasures for Facilities, and SPB Issuance 6–97, entitled National Policy on Technical Surveillance Countermeasures.

§ 2004.14 Emergency authority.

Agency heads may prescribe special provisions for the dissemination, transmittal, destruction, and safeguarding of classified information during military operations or other emergency situations.

APPENDIX A TO PART 2004—OPEN STORAGE AREAS

This Appendix describes the construction standards for open storage areas.

1. *Construction.* The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.

2. *Doors.* Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three-position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.

3. *Vents, ducts, and miscellaneous openings.* All vents, ducts, and similar openings in excess of 96 square inches (and over 6 inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sound baffles, or an intrusion detection system.

4. *Windows.*

a. All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

b. Windows at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area.)

APPENDIX B TO PART 2004—FOREIGN GOVERNMENT INFORMATION

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, or other obligation. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I–69 and I–70. To the extent practical,

and to facilitate its control, foreign government information should be stored separately from other classified information. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government.

1. *Top Secret*. Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

2. *Secret*. Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

3. *Confidential*. Records need not be maintained for foreign government Confidential information unless required by the originator.

4. *Restricted and other foreign government information provided in confidence*. In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government ''Restricted,'' ''Designated,'' or unclassified provided in confidence), such information must be classified under E.O. 12958. The receiving agency, or a receiving U.S. contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, shall provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to US CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for US CONFIDENTIAL information, the following requirements shall be met:

a. Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be marked, ''This document contains (insert name of country) (insert classification level) information to be treated as US (insert classification level).'' The notation, ''Modified Handling Authorized,'' may be added to either the foreign or U.S. markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

b. Documents shall be provided only to those who have an established need-to-know, and where access is required by official duties;

c. Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

d. Documents shall be stored in such a manner so as to prevent unauthorized access;

e. Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

5. *Third-country transfers*. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.