§ 2004.10 Loss, possible compromise or unauthorized disclosure.

(a) General. Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) Cases involving information originated by a foreign government or another U.S. government agency. Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) Inquiry/investigation and corrective actions. Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) Department of Justice and legal counsel coordination. Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with—

1. The Department of Justice, and
2. The legal counsel of the agency where the individual responsible is assigned or employed.

§ 2004.11 Special access programs.

(a) General. The safeguarding requirements of this Directive may be enhanced for information in Special Access Programs (SAP), established under the provisions of Section 4.4 of E.O.
§ 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.


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.


Agency heads may prescribe special provisions for the dissemination, transmission, 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. 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. 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,