may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(1) *Combinations.* Combinations to locks used to secure vaults, open storage areas, and security containers that are approved for the safeguarding of classified information shall be protected in the same manner as the highest level of classified information that the vault, open storage area, or security container is used to protect.

(2) *Computer and information system passwords.* Passwords shall be protected in the same manner as the highest level of classified information that the computer or system is certified and accredited to process. Passwords shall be changed on a frequency determined to be sufficient to meet the level of risk assessed by the agency.

(b) *Reproduction.* Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:

(1) Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

(2) Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

(3) Copies of classified information shall be subject to the same controls as the original information; and

(4) The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

(c) *Forms.* The use of standard forms prescribed in Subpart H of this part is mandatory for all agencies that create and/or handle national security information.

(d) *Redaction*—(1) *Policies and procedures.* Classified information may be subject to loss, compromise, or unauthorized disclosure if it is not correctly redacted. Agencies shall establish policies and procedures for the redaction of classified information from documents intended for release. Such policies and procedures require the approval of the agency head and shall be sufficiently detailed to ensure that redaction is performed consistently and reliably, using only approved redaction methods that permanently remove the classified information from copies of the documents intended for release. Agencies shall ensure that personnel who perform redaction fully understand the policies, procedures, and methods and are aware of the vulnerabilities surrounding the process.

(2) *Technical guidance for redaction.* Technical guidance concerning appropriate methods, equipment, and standards for the redaction of classified electronic and optical media shall be issued by NSA.

§ 2001.46 Transmission.

(a) *General.* Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Directive.

(b) *Dispatch.* Agency heads shall establish procedures which ensure that:

(1) All classified information physically transmitted outside facilities shall be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible. Intended recipients shall be identified by name only as part of an attention line. The following exceptions apply:

(i) If the classified information is an internal component of a packable item of equipment, the outside shell or body

may be considered as the inner enclosure provided it does not reveal classified information;

(ii) If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;

(iii) If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;

(iv) Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

(v) When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF–P–110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(c) *Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.*

(1) *Top Secret.* Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort with Top Secret clearance; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other cleared or uncleared commercial carrier.

(2) *Secret.* Secret information shall be transmitted by:

(i) Any of the methods established for Top Secret; U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature block on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited; and

(ii) Agency heads may, when a requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (39 CFR. Chapter I) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of classified information. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

(3) *Confidential.* Confidential information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, when the recipient is a U.S. Government facility, the Confidential information may be transmitted via U.S. First Class Mail. However, Confidential information shall not be transmitted to government contractor facilities via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked

to indicate that the information is not to be forwarded, but is to be returned to sender. The use of streetside mail collection boxes is prohibited.

(d) *Transmission methods to a U.S. Government facility located outside the U.S.* The transmission of classified information to a U.S. Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

(e) *Transmission of U.S. classified information to foreign governments.* Such transmission shall take place between designated government representatives using the government-to-government transmission methods described in paragraph (d) of this section or through channels agreed to by the National Security Authorities of the two governments. When classified information is transferred to a foreign government or its representative a signed receipt is required.

(f) *Receipt of classified information.* Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. As noted in paragraph (e) of this section, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.

§ 2001.47 Destruction.

Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Agencies shall comply with the destruction equipment standard stated in § 2001.42(b) of this Directive.

§ 2001.48 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 U.S. 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) *Reports to ISOO.* In accordance with section 5.5(e)(2) of the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:

(1) Is reported to oversight committees in the Legislative branch;

(2) May attract significant public attention;

(3) Involves large amounts of classified information; or