

§ 1312.29 Destruction.

The destruction of classified material will be accomplished under the direction of the TSCO or the appropriate ATSCO, who will assure that proper accountability records are kept. Classified official record material will be processed to the Information Systems and Technology, Records Management Office, Office of Administration, NEOB Room 5208, in accordance with OMB Manual Section 540. Classified non-record material will be destroyed as soon as it becomes excess to the needs of the office. The following destruction methods are authorized:

(a) *Shredding.* Using the equipment approved for that purpose within OMB offices. Shredders will not accommodate typewriter ribbons or cassettes. Shredding is the only authorized means of Destroying Top Secret material.

(b) *Burn bag.* Classified documents, cassettes, ribbons, and other materials at the Secret level or below, not suitable for shredding, may be destroyed by using burn bags, which can be obtained from the supply store. They will be disposed of as follows:

(1) *OEOB.* Unless on an approved list for pick-up of burn bags, all other burn bags should be delivered to Room 096, OEOB between 8:00 a.m. and 4:30 p.m. Burn bags are not to be left in hallways.

(2) *NEOB.* Hours for delivery of burn bag materials to the NEOB Loading Dock Shredder Room are Monday through Friday from 8:00 a.m. to 9:30 a.m.; 10:00 a.m. to 11:00 a.m.; 11:45 a.m. to 1:30 p.m. and 2:00 p.m. to 3:30 p.m. The phone number of the Shredder Room is 395-1593. In the event the Shredder Room is not manned, do not leave burn bags outside the Shredder Room as the security of that material may be compromised.

(3) Responsibility for the security of the burn bag remains with the OMB office until it is handed over to the authorized representative at the shredder room. Accountability records will be adjusted after the burn bags have been delivered. Destruction actions will be recorded on OMB Form 87 by the division TSCO or by the appropriate ATSCO at the time the destruction is accomplished or at the time the burn bag is delivered to the U.D. Officer.

(c) *Technical guidance.* Technical guidance concerning appropriate methods, equipment, and standards for destruction of electronic classified media, processing equipment components and the like, may be obtained by submitting all pertinent information to NSA/CSS Directorate for Information Systems Security, Ft. Meade, Maryland 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

§ 1312.30 Loss or possible compromise.

Any person who has knowledge of the loss or possible compromise of classified information shall immediately secure the material and then report the circumstances to the EOP Security Officer. The EOP Security Officer will immediately initiate an inquiry to determine the circumstances surrounding the loss or compromise for the purpose of taking corrective measures and/or instituting appropriate administrative, disciplinary, or legal action. The agency originating the information shall be notified of the loss or compromise so that the necessary damage assessment can be made.

§ 1312.31 Security violations.

(a) A security violation notice is issued by the United States Secret Service when an office/division fails to properly secure classified information. Upon discovery of an alleged security violation, the USSS implements their standard procedures which include the following actions:

(1) Preparation of a Record of Security Violation form;

(2) When a document is left on a desk or other unsecured area, the officer will remove the classified document(s) and deliver to the Uniformed Division's Control Center; and

(3) Where the alleged violation involves an open safe, the officer will remove one file bearing the highest classification level, annotate it with his or her name, badge number, date and time, and return the document to the

safe, which will then be secured. A description of the document will be identified in the Record of Security Violations and a copy of the violation will be left in the safe.

(b) *Office of record.* The EOP Security Office shall serve as the primary office of record for OMB security violations. Reports of violations will remain in the responsible individual's security file until one year after the individual departs the Executive Office of the President, at which time all violation reports will be destroyed.

(c) *Compliance.* All Office of Management and Budget employees will comply with this section. Additionally, personnel on detail or temporary duty will comply with this section, however, their parent agencies will be provided with a copy of any security violation incurred during their period of service to OMB.

(d) *Responsibilities for processing security violations—(1) EOP Security Officer.* The EOP Security Officer shall provide OMB with assistance regarding Agency security violations. Upon receipt of a Record of Security Violation alleging a security violation, the EOP Security Officer shall:

(i) Prepare a memorandum to the immediate supervisor of the office/division responsible for the violation requesting that an inquiry be made into the incident. Attached to the memorandum will be a copy of the Record of Security Violation form. The receiving office/division will prepare a written report within five working days of its receipt of the Security Officer's memorandum.

(ii) Provide any assistance needed for the inquiry conducted by the office/division involved in the alleged violation.

(iii) Upon receipt of the report of inquiry from the responsible office/division, the EOP Security Officer will:

(A) Consult with the OMB Associate Director (or Assistant Director) for Administration and the General Counsel;

(B) Determine if a damage assessment report is required. A damage assessment will be made by the agency originating the classified information, and will be prepared after it has been determined that the information was accessed without authorization; and

(C) Forward the report with a recommendation to the OMB General Counsel.

(2) *Immediate supervisors.* Upon receipt of the EOP Security Officer's security violation memorandum, the immediate supervisor will make an inquiry into the alleged incident, and send a written report of inquiry to the EOP Security Officer. The inquiry should determine, and the related report should identify, at a minimum:

(i) Whether an actual security violation occurred;

(ii) The identity of the person(s) responsible; and

(iii) The probability of unauthorized access.

(3) Deputy Associate Directors (or the equivalent) will:

(i) Review and concur or comment on the written report; and

(ii) In conjunction with the immediate supervisor, determine what action will be taken to prevent, within their area of responsibility, a recurrence of the circumstances giving rise to the violation.

(e) *Staff penalties for OMB security violations.* When assessing penalties in accordance with this section, only those violations occurring within the calendar year (beginning January 1) will be considered. However, reports of all previous violations remain in the security files. These are the standard violation penalties that will be imposed. At the discretion of the Director or his designee, greater or lesser penalties may be imposed based upon the circumstances giving rise to the violation, the immediate supervisor's report of inquiry, and the investigation and findings of the EOP Security Officer and/or the OMB Associate Director (or Assistant Director) for Administration.

(1) First violation:

(i) Written notification of the violation will be filed in the responsible individual's security file; and

(ii) The EOP Security Officer and/or the Associate Director (or Assistant Director) for Administration will consult with the respective immediate supervisor, and the responsible individual will be advised of the penalties that may be applied should a second violation occur.

(2) Second violation:

(i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director (or Assistant Director) for Administration will consult with the respective Deputy Associate Director (or the equivalent) and immediate supervisor and the responsible individual who will be advised of the penalties that may be applied should a third violation occur; and

(iii) A letter of Warning will be placed in the Disciplinary Action file maintained by the Office of Administration, Human Resources Management Division.

(3) Third violation:

(i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director (or Assistant Director) for Administration will consult with the OMB Deputy Director, General Counsel, the respective Deputy Associate Director (or equivalent), and the immediate supervisor and the responsible individual who will be advised of the penalties that may be applied should a fourth violation occur; and

(iii) A Letter of Reprimand will be placed in the Disciplinary Action file maintained by the OA/HRMD.

(4) Fourth violation:

(i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director (or Assistant Director) for Administration will consult with the OMB Director, Deputy Director, General Counsel, the respective Deputy Associate Director (or the equivalent), and immediate supervisor;

(iii) The responsible individual may receive a suspension without pay for a period not to exceed 14 days; and

(iv) The responsible individual will be advised that future violations could result in the denial of access to classified material or other adverse actions as may be appropriate, including dismissal.

Subpart C—Mandatory Declassification Review

§ 1312.32 Purpose and authority.

Other government agencies, and individual members of the public, frequently request that classified information in OMB files be reviewed for possible declassification and release. This subpart prescribes the procedures for such review and subsequent release or denial. It is issued under the authority of Executive Order 12958 (60 FR 19825, 3 CFR, 1995 Comp., p. 333), as implemented by Information Security Oversight Office Directive No. 1 (32 CFR part 2001).

§ 1312.33 Responsibility.

All requests for the mandatory declassification review of classified information in OMB files should be addressed to the Associate Director (or Assistant Director) for Administration, who will acknowledge receipt of the request. When a request does not reasonably describe the information sought, the requester shall be notified that unless additional information is provided, or the scope of the request is narrowed, no further action will be taken. All requests will receive a response within 180 days of receipt of the request.

§ 1312.34 Information in the custody of OMB.

Information contained in OMB files and under the exclusive declassification jurisdiction of the office will be reviewed by the office of primary interest to determine whether, under the declassification provisions of the Order, the requested information may be declassified. If so, the information will be made available to the requestor unless withholding is otherwise warranted under applicable law. If the information may not be released, in whole or in part, the requestor shall be given a brief statement as to the reasons for denial, a notice of the right to appeal the determination to the Deputy Director, OMB, and a notice that such an appeal must be filed within 60 days in order to be considered.