

records. Classified information approved for destruction shall be destroyed by either burning, melting, chemical decomposition, pulping, mulching, pulverizing, cross-cut shredding or other mutilation in the presence of appropriately cleared and authorized persons. The method of destruction *must* preclude recognition or reconstruction of the classified information. The residue from cross-cut shredding of Top Secret, Secret, and Confidential classified, non-Communications Security (COMSEC), information contained in paper media may not exceed  $\frac{3}{32}$ " by  $\frac{1}{2}$ " with a  $\frac{1}{64}$ " tolerance.

(a) *Diskettes or Floppy Disks.* Diskettes or floppy disks containing information or data classified up to and including Top Secret may be destroyed by the use of an approved degausser, burning, pulverizing, and chemical decomposition, or by first reformatting or reinitializing the diskette then physically removing the magnetic disk from its protective sleeve and using an approved cross-cut shredder to destroy the magnetic media. Care must be exercised to ensure that the destruction of magnetic disks does not damage the cross-cut shredder. The residue from such destruction, however, may not exceed  $\frac{1}{32}$ " by  $\frac{1}{2}$ " with a  $\frac{1}{64}$ " tolerance. The destruction of classified COMSEC information on diskettes or floppy disks may only be effected by burning followed by crushing of the ash residue.

(b) *Hard Disks.* Hard disks, including removable hard disks, disk packs, drums or single disk platters that contain classified information must first be degaussed prior to physical destruction. The media must be destroyed by incineration, chemical decomposition or the entire magnetic disk pack, drum, or platter recording surface must be obliterated by use of an emery wheel or disk sander.

(c) *Approval of Use of Mulching and Cross-cut Shredding Equipment.* Prior to obtaining mulching or cross-cut shredding equipment, the Departmental Director of Security shall approve the use of such equipment.

(d) *Use of Burnbags.* Any classified information to be destroyed by burning shall be torn and placed in opaque containers, commonly designated as burnbags, which shall be clearly and

distinctly labeled "BURN" or "CLASSIFIED WASTE". Burnbags awaiting destruction are to be protected by security safeguards commensurate with the classification or control designation of the information involved.

(e) *Records of Destruction.* Appropriate accountability records shall be maintained on TD F 71-01.17 (Classified Document Certificate of Destruction) to reflect the destruction of all Top Secret and Secret information. As deemed necessary by the originator, or as required by special regulations, the TD F 71-01.17 shall be executed for the destruction of information classified Confidential or marked Limited Official Use. TD F's 71-01.17 shall be maintained for a three-year period after which the form may be destroyed. No record of the actual destruction of the TD F 71-01.17 is required.

(f) *Destruction of non-record Classified Information.* Non-record classified information such as extra copies and duplicates, including shorthand notes, preliminary drafts, used carbon paper and other material of similar temporary nature, shall also be destroyed by burning, mulching, or cross-cut shredding as soon as it has served its purpose, but no records of such destruction need be maintained.

[55 FR 1644, Jan. 17, 1990; 55 FR 5118, Feb. 13, 1990]

### § 2.37 National Security Decision Directive 197.

National Security Decision Directive 197, Reporting Hostile Contacts and Security Awareness, provides that United States Government employees are responsible for reporting to their designated security officer:

(a) Any suspected or apparent attempt by persons, regardless of nationality, to obtain unauthorized access to classified national security information, sensitive or proprietary information or technology and/or;

(b) Instances in which they feel they are being targeted for possible exploitation. Contacts with representatives of designated countries of concern identified in § 2.43(f) which involve requests for information which are not ordinarily provided in the course of an employee's job, regular or daily activity, and/or which might possibly lead

## § 2.38

to further requests for access to sensitive, proprietary or classified information or technology, are to be reported to designated security officers. Reports of such contacts are to be forwarded by the designated security officer to the Departmental Director of Security for appropriate action and coordination.

### Subpart E—Implementation and Review

#### § 2.38 Departmental management.

(a) The Assistant Secretary (Management) shall:

(1) Enforce the Order, the Directive and this regulation, and establish, coordinate and maintain active training, orientation and inspection programs for employees concerned with classified information.

(2) Review suggestions and complaints regarding the administration of this regulation.

(b) Pursuant to Treasury Directive 71-08, "Delegation of Authority Concerning Physical Security Programs", the Departmental Director of Security shall:

(1) Review all bureau implementing regulations prior to publication and shall require any regulation to be changed, if it is not consistent with the Order, the Directive or this regulation.

(2) Have the authority to conduct on-site reviews of bureau physical security programs and information security programs as they pertain to each Treasury bureau and to require such reports, information and assistance as may be necessary, and

(3) Serve as the principal advisor to the Assistant Secretary (Management) with respect to Treasury physical and information security programs.

#### § 2.39 Bureau administration.

Each Treasury bureau and the Departmental Offices shall designate, in writing to the Departmental Director of Security, an officer or official to direct, coordinate and administer its physical security and information security programs which shall include active oversight to ensure effective implementation of the Order, the Directive, this regulation. Bureaus and the Departmental Offices shall revise their

## 31 CFR Subtitle A (7-1-05 Edition)

existing implementing regulation on national security information to ensure conformance with this regulation. Time frames for bureau and Departmental Offices implementation shall be established by the Departmental Director of Security.

#### § 2.40 Emergency planning [4.1(b)].

Each Treasury bureau and the Departmental Offices shall develop plans for the protection, removal, or destruction of classified information in case of fire, natural disaster, civil disturbance, or possible enemy action. These plans shall include the disposition of classified information located in foreign countries.

#### § 2.41 Emergency authority [4.1(b)].

The Secretary of the Treasury may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

#### § 2.42 Security education [5.3(a)].

Each Treasury bureau that creates, processes or handles national security information, including the Departmental Offices, is required to establish a security education program. The program shall be sufficient to familiarize all necessary personnel with the provisions of the Order, the Directive, this regulation and any other implementing directives and regulations to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

(a) *Briefing of Employees.* All new employees concerned with classified information shall be afforded a security briefing regarding the Order, the Directive and this regulation and sign a security agreement as required in § 2.22(c). Employees concerned with sensitive compartmented information shall be required to read and also sign a security agreement. Copies of applicable laws and pertinent security regulations setting forth the procedures for the protection and disclosure of classified information shall be available for all new employees afforded a security