

cross-cut shredder. The residue from such destruction, however, may not exceed 1/32" by 1/2" with a 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 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",