

§ 2.33

(4) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of sensitive compartmented information has occurred.

§ 2.33 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for protecting it from persons not authorized access, i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know. This includes keeping classified documents under constant observation and turned face-down or covered when not in use and securing such information in approved security equipment or facilities whenever it is not under the direct supervision of authorized persons. In all instances, such protective means must meet accountability requirements prescribed by the Department.

§ 2.34 Inspections [4.1(b)].

Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. Security officers shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by this regulation and any bureau implementing regulation are in effect at all times. At a minimum such checks shall ensure that all classified information is stored in approved security containers, including removable storage media, e.g., floppy disks used by word processors that contain classified information; burn bags, if utilized, are either stored in approved security containers or destroyed; and classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 2.35 Security violations.

Any individual, at any level of employment, determined to have been responsible for the unauthorized release or disclosure or potential release or

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

disclosure of classified national security information, whether it be knowingly, willfully or through negligence, shall be notified on TD F 71-21.1 (Record of Security Violation) that his or her action is in violation of this regulation, the Order, the Directive, and Executive Order 10450, as amended. Treasury Directive 71-04, entitled, "Administration of Security Violations" sets forth provisions concerning security violations which shall apply to each Treasury employee and persons under contract or subcontract to the Department authorized access to Treasury classified national security information.

(a) Repeated abuse of the classification process, either by unnecessary or over-classification, or repeated failure, neglect or disregard of established requirements for safeguarding classified information by any employee shall be grounds for appropriate adverse or disciplinary action. Such actions may include, but are not necessarily limited to, a letter of warning, a letter of reprimand, suspension without pay, or dismissal, as appropriate in the particular case, under applicable personnel rules, regulations and procedures. Where a violation of criminal statutes may be involved, any such case shall be promptly referred to the Department of Justice.

(b) After an affirmative adjudication of a security violation, and as the occasion demands, reports of accountable security violations shall be placed in the employee's personnel security file, and as appropriate, in the employee's official personnel folder. The security official of the office or bureau concerned shall recommend to the respective management official or bureau head that disciplinary action be taken when such action is indicated.

§ 2.36 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Title 44, United States Code, Chapters 21 and 33, which govern disposition of Federal

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