

## Office of the Secretary of the Treasury

## § 2.34

(3) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(4) An assessment of the possible advantage to foreign powers resulting from the compromise.

(5) An assessment of whether,

(i) The classification of the information involved should be continued without change;

(ii) The specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained;

(iii) Downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change, and

(6) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(d) *System for Control of Damage Assessments.* Each Treasury bureau and the Departmental Offices shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in § 2.32(a) and that records are maintained in a manner that facilitates their retrieval and use within the Department.

(e) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, the Departmental Director of Security shall advise the other affected agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment and Treasury components will provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(2) Whenever a compromise of United States classified information is the result of actions taken by foreign nationals, by foreign government officials, or by United States nationals in the employ of international organizations, the agency performing the damage assessment shall endeavor to ensure through

appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(3) Whenever an action is contemplated against any person believed responsible for the loss or compromise of classified information, damage assessments shall be coordinated with appropriate legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, coordination shall be made with the Department of Justice.

(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

### § 2.35

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 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,

### 31 CFR Subtitle A (7-1-02 Edition)

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