

§ 2.39

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 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

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

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 briefing. All employees given a security briefing shall be required to sign a TD F 71-01.16 (Physical Security Orientation Acknowledgment) which shall be maintained on file as determined by respective office or bureau security officials.

(b) [Reserved]

Subpart F—General Provisions

§ 2.43 Definitions [6.1].

(a) *Authorized Person.* Those individuals who have a “need-to-know” the classified information involved and have been cleared for the receipt of such information. Responsibility for determining whether individuals’ duties require that they possess, or have access to, any classified information and whether they are authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipients.

(b) *Compromise.* The loss of security enabling unauthorized access to classified information. Affected information or material is not automatically declassified.

(c) *Confidential Source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.