

§ 2.29

is based on the need for reviewing classified materials while enroute. Travelers are responsible for reviewing and familiarizing themselves with required classified materials, under appropriately secure circumstances, in advance of their travel and not during such travel.

(iv) In order to avoid unnecessary delays in the screening process prior to boarding commercial air carriers, the traveler shall have in his or her possession written authorization, on Treasury or bureau letterhead, to transport classified information and either an identification card or credential bearing both a photograph and descriptive data. Courier authorizations shall be signed by an appropriate security representative authorized to direct official travel. This courier authorization, along with official travel orders, shall, in most instances, permit the individual to exempt the classified information from inspection. If difficulty is encountered, the traveler should tactfully refuse to exhibit or disclose the classified information to inspection and should insist on the assistance of the local United States diplomatic representative at the port of entry or departure.

(v) Upon completion of the visit, the traveler shall have the information returned to his or her office by approved means. All Top Secret and Secret classified information, including teletype messages transported for the purpose of the visit shall be accounted for. It is highly recommended that Confidential and Limited Official Use information also be accounted for. If any Top Secret or Secret classified items are left with the office being visited for its retention and use, the individual shall obtain a receipt.

[55 FR 1644, Jan. 17, 1990, as amended at 55 FR 50321, Dec. 6, 1990]

§ 2.29 Telecommunications and computer transmissions.

Classified information shall not be communicated by telecommunications or computer transmissions except as may be authorized with respect to the transmission of classified information over authorized secure communications circuits or systems.

31 CFR Subtitle A (7-1-04 Edition)

§ 2.30 Special access programs [1.2(a) and 4.2(a)].

Only the Secretary of the Treasury may create or continue a special access program if:

(a) Normal management and safeguarding procedures do not limit access sufficiently; and

(b) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2.31 Reproduction controls [4.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electronically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret, Confidential and Limited Official Use documents may be reproduced to the extent required by operational needs.

(c) Reproductions of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for possible declassification.

§ 2.32 Loss or possible compromise [4.1(b)].

(a) *Report of Loss or Possible Compromise.* Any Treasury employee who has knowledge of the loss or possible compromise or classified information shall immediately report the circumstances to their designated office or bureau security officer who shall take appropriate action to assess the degree of damage. In turn, the Departmental Director of Security shall be immediately notified by the affected office or bureau security officer of such reported loss or possible compromise. The Departmental Director of Security shall also notify the department or agency which originated the information and any other interested department or agency so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the loss or possible compromise. Compromises