AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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.

§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 may occur through espionage, unauthorized disclosures to the press or other members of the public, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Inquiry.* The Departmental Director of Security shall notify the Assistant Secretary (Management) who shall then direct an immediate inquiry to be conducted for the purpose of taking corrective measures and assessing damages. Based on the results of this inquiry, it may be deemed appropriate to notify the Inspector General who shall determine whether the Office of the Inspector General or a Treasury bureau will conduct any additional investigation. Upon completion of the investigation by the Inspector General, the Inspector General shall recommend to the Assistant Secretary (Management) and concurrently to the Departmental Director of Security, the appropriate administrative, disciplinary, or legal action to be taken based upon jurisdictional authority of the Treasury components involved.

(c) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date and circumstances of the compromise.

(2) Classification and description of the specific information which has been lost.