AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

or Departmental Offices central repository for security combinations. Part 2 shall have the highest level of classified information, stored in the security equipment concerned, annotated in both the top and bottom border areas of the completed SF 700. Part 2A shall have the highest level of classified information, stored in the security equipment concerned, annotated in the blank space immediately above the word, ''WARNING'' which appears on the SF 700. The completion of the SF 700 or Treasury Form 4032 does not constitute a classification action but serves as an administrative requirement to ensure the protection of classified information stored in such security equipment. SF 700 shall be utilized on all security equipment used for storing information bearing the control legend ''Limited Official Use''. The designated security officer in each Treasury bureau and the Departmental Offices may prescribe supplementary use of the SF 700 to apply to other authorized legends approved by the Department for officially limited information, as warranted.

(c) *Keys.* The designated security officer in each Treasury bureau and the Departmental Offices shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the information being protected by the padlock.

(d) *Classified Document Cover Sheets.* Classified document cover sheets alert personnel that documents or folders are classified and require protection from unauthorized scrutiny. Individuals who prepare or package classified documents are responsible for affixing the appropriate document cover sheet. Orange Standard Form 703 (Top Secret Cover Sheet), red SF 704 (Secret Cover Sheet) and blue SF 706 (Confidential Cover Sheet) are the only authorized cover sheets for collateral classified information. The national stock numbers of these cover sheets are as follows: SF 703, 7540–01–213–7901; SF 704, 7540–01–213–7902; and SF 705, 7540–01–213–7903. In order to maintain the integrity of the color coding process the photocopying and use of non-color coded classified document cover sheets is prohibited. Bureaus and offices shall maintain a supply of classified document cover sheets appropriate for their needs. Classified document cover sheets are designed to be reused and will be removed before classified information is filed to conserve filing space and prior to the destruction of classified information. Document cover sheets are to be used to shield classified documents while in use and particularly when the transmission is made internally within a headquarters by courier, messenger or by personal contact. File folders containing classified information should be otherwise marked, e.g., at the top and bottom of the front and back covers, to indicate the overall classification of the contents rather than permanently affixing the respective classified document cover sheet. Treasury Directive 71–02 provides for the use of a green cover sheet, TD F 71–01.6 (Limited Official Use Document Cover Sheet) for information bearing the control legend ''Limited Official Use''. Bureaus or offices electing to create and use other cover sheets for officially limited information must obtain prior written approval from the Departmental Director of Security.

(e) *Activity Security Checklist.* Standard Form 701 (Activity Security Checklist) provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability in the event that irregularities are discovered. Bureaus and the Departmental Offices may include additional information on the SF 701 to suit their unique needs. The SF 701, available through normal supply channels has a national stock number of 7540–01–213–7900. It shall be the only form used in situations that call for use of an activity security checklist. Completion, storage and disposition of SF 701 will be determined by each bureau and the Departmental Offices.

§ 2.28 Transmittal [4.1(b)].

(a) *Preparation.* Classified information to be transmitted outside of a Treasury facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or

envelope plainly marked with the assigned security classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. Whenever classified material is to be transmitted and the size of the material is not suitable for use of envelopes or similar wrappings, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings. Material used for packaging such bulk classified information shall be of sufficient strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to facilitate detection of any tampering therewith.

(b) *Receipting.* A receipt, Treasury Department Form 71–01.5 (Classified Document Record of Transmittal), shall be enclosed in the inner cover, except that Confidential and Limited Official Use information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee and describe the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Within a Treasury facility, such information may be transmitted between offices by direct contact of the officials concerned in a single sealed opaque envelope with no security classification category being shown on the outside of the envelope. Classified information shall never be delivered to unoccupied offices or rooms. Senders of classified information should maintain appropriate records of outstanding receipts for which return of the original signed copy is still pending. TD F's 71–01.5 shall be maintained for a three year period after which they may be destroyed. No record of the actual destruction of the TD F 71–01.5 is required.

(c) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a Treasury facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for that purpose, e.g., Defense Courier Service, or over authorized secure communications circuits. Top Secret information may *not* be sent via registered mail.

(d) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) *The 50 States, District of Columbia and Puerto Rico.* Secret information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information, by the United States Postal Service registered mail or express mail service; or by protective services provided by United States air or surface commercial carriers under such conditions as may be prescribed by the Departmental Director of Security. United States Postal Service express mail service shall be used only when it is the most effective means to accomplish a mission within security, time, cost and accountability constraints. To ensure direct delivery to the addressee, the ''Waiver of Signature and Indemnity'' block on the United States Postal Service Express Mail Label 11–B may not be executed under any circumstances. All Secret express mail shipments are to be processed through mail distribution centers or delivered directly to a United States Postal Service facility or representative. The use of external (street side) express mail collection boxes is prohibited. Only the express mail services of the United States Postal Service are authorized.

(2) *Other Areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2.28(d)(1) by one of the means established for Top Secret information, or by United States registered mail through Military Postal Service facilities provided that the information does not at any time pass out of United States citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard United States Government owned and United States Government contract vehicles or aircraft, ships of the United States Navy, civil service manned United States Naval ships, and ships of United States Registry. Operators of

vehicles, captains or masters of vessels, and pilots of aircraft who are United States citizens, and who are appropriately cleared, may be designated as escorts. Secret information may not be sent via certified mail.

(e) *Transmittal of Confidential and Limited Official Use Information.* Confidential and Limited Official Use information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and United States territories or possessions by one of the means established for higher classifications, or by the United States Postal Service registered mail. Outside these areas, confidential and Limited Official Use information shall be transmitted only as is authorized for higher classifications. Confidential and Limited Official Use information may not be sent via certified mail.

(f) *Hand Carrying of Classified Information in Travel Status*—(1) *General Provisions.* Personnel in travel status shall physically transport classified information across international boundaries only when absolutely essential. Whenever possible, and when time permits, the most desirable way to transmit classified information to the location being visited is by other authorized means identified in § 2.28 (c), (d) and (e). The physical transportation of classified information on non-United States flag aircraft should be avoided if possible. Treaury Directive 71–03, ''Screening of Airline Passengers Carrying Classified Information or Material'' provides specifics on the requirements for transporting classified information.

(2) *Specific Safeguards.* If it is determined that the transportation of classified information by an individual in travel status is in the best interest of the United States Government, the following specific safeguards shall be fulfilled:

(i) Classified information shall be in the physical possession of the individual and shall have adequate safeguards at all times if proper storage at a United States Government facility is not available. Under no circumstances shall classified information be stored in a hotel safe or room, locked in automobiles, private residences, train compartments, or any vehicular detachable storage compartments.

(ii) An inventory of all Top Secret classified information, including teletype messages, shall be made prior to departure and a copy of same shall be retained by the traveller's office until the traveller's return at which time all Top Secret classified information shall be accounted for. These same procedures are recommended for information classified Secret, Confidential or Limited Official Use.

(iii) Classified information shall never be displayed or used in any manner in public conveyances or rooms. First class or business travel is not authorized when the justification for commercially available transportation 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.

§ 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.