12 FAM 530
STORING AND SAFEGUARDING CLASSIFIED MATERIAL

(TL:DS-81; 01-31-2002)

12 FAM 531 GENERAL

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Store classified material only in a manner that conforms to the provisions of this section.

b. Whenever classified material is not under the personal control and observation of an authorized person, store it in an approved locked container under the conditions cited in this section. At Foreign Service posts, open storage of classified material in a vault, except material in sealed diplomatic pouches, is not allowed unless specifically authorized in writing by DS/CIS/IST. Domestically, for the Department of State, contact DS/CIS/IST regarding open storage. Domestically within A.I.D., contact IG/SEC.

c. Classified material in data and word processing systems, to include magnetic storage media, will be used, held, processed, or stored only under conditions which will prevent unauthorized persons from gaining access to it. The DS Office of Information Security Technology (DS/CIS/IST) establishes requirements for the protection of classified information resident on automated information systems (AIS). Within A.I.D., IG/SEC establishes these requirements.

d. Responsibility for the secure storage of classified material in message distribution lockers (MDLs) rests with appropriate personnel from the office to which the locker is assigned. Employees must treat the combinations to MDLs the same as the combinations to other security containers where classified material may be stored. Employees must classify combinations to MDLs no lower than the highest level of classified material authorized for storage in the MDL. When an MDL is found unsecured, whether empty or not, employees must consider the combination to the MDL compromised.

e. The Department has developed and approved revised security standards

for the storage of classified material at facilities abroad. These standards were coordinated with the Overseas Security Policy Group and apply to all personnel and facilities under the authority of the chief of mission. (See 12 FAM 531.1 and 12 FAM 531.2.)

f. At Foreign Service posts, material relating to intelligence sources and methods is protected under separate guidelines.

g. Classified material should not be stored at a facility outside the chancery, consulate, etc., merely for convenience. In order to store classified material, a post must demonstrate to the regional security officer (RSO) a legitimate need to have material at a given location, as well as provide a justification for the level of classified material to be stored.

h. Separately located Voice of America (VOA) stations will not store classified information. Arrangements have been made for staff to store and read the information at embassies and consulates. The material may be taken from the storage site to the VOA facility during working hours, but must either be returned at close of business or destroyed with an approved device. Sensitive But Unclassified (SBU) material may continue to be stored at VOA facilities.

i. Regulations concerning storage requirements for authorized consultants and contractors engaged in work involving classified information are covered in subchapter 12 FAM 570.

12 FAM 531.1 Top Secret Storage

12 FAM 531.1-1 Domestic

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Top Secret documents must be stored in a General Services Administration (GSA)-approved container with a GSA-approved, built-in, three-position, dial-type combination lock, located either in a DS-approved alarmed area or in a building controlled by cleared U.S. citizen personnel on a 24-hour basis. For the Department of State, DS/CIS/IST must approve any exceptions. Within A.I.D., IG/SEC approves exceptions.

12 FAM 531.1-2 At Foreign Service Posts

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

See 12 FAH-6, OSPB Security Standards and Policy Handbook, for storage requirements.

12 FAM 531.2 Secret and Confidential Storage

12 FAM 531.2-1 Domestic

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Secret and Confidential material may be stored:

(1) In the same manner as authorized for Top Secret information; or

(2) In a GSA-approved container with a GSA-approved, built-in, three-position, dial-type combination lock; or

(3) In a barlock cabinet equipped with a GSA-approved three-position, dial-type, changeable, combination padlock located either in a DS-approved alarmed area or in a building controlled by cleared U.S. citizen personnel on a 24-hour basis.

12 FAM 531.2-2 Foreign Service Posts

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

See 12 FAH-6, OSPB Security Standards and Policy Handbook, for storage requirements.

12 FAM 532 LOCKS

12 FAM 532.1 Electronically and Manually Activated Locks

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Electronically activated locks (for example, cypher and magnetic strip card lock) and simplex locks do not afford the required degree of protection for classified information and may not be used as a substitute for the locks prescribed in 12 FAM 531.1 and 12 FAM 531.2.

12 FAM 532.2 Changing Combinations

12 FAM 532.2-1 Individuals Authorized to Change Combinations

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Combinations to security containers and vaults will be changed only by individuals having an appropriate security clearance.

(1) Domestically, combinations may be changed by individuals approved by the cognizant foreign affairs agency security office (see 12 FAM 511.1).

(2) Abroad, regional security officers and communications programs officers (for combinations within the post communications center (PCC)) will ensure combinations.

12 FAM 532.2-2 When Combinations Will Be Changed

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Combinations will be changed under the following circumstances:

(1) When the lock is initially put into use;

(2) When an employee knowing the combination terminates employment or is permanently transferred to duties which no longer require employee's access;

(3) Upon knowledge or suspicion that the combination has become known to an unauthorized person;

(4) Whenever a security violation results from an unsecured security container;

(5) At least once every 12 months, except for computer room and communication area vault doors, which must be changed every 6 months; or

(6) When containers are moved from active to inactive service, reset the combination lock domestically to the factory combination (50-25-50) and abroad reset the lock to the post security combination (PSC). The PSC is provided by the post security officer. When

containers are moved from inactive to active service, reset combination padlocks to a combination of 10-20-30. See 12 FAM 539.1, paragraph g, for further information.

12 FAM 532.2-3 Recording Combination Changes

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Combinations must be recorded on Form SF-700, Security Container Information. (See 12 FAM 532 Exhibit 532.2-3.) Records of combinations (containers, built-in combination locks, vault doors, padlocks, MDLs, etc.) will be classified at the highest level of classified material to be stored in the security container.

b. At Foreign Service posts such cards must be completed in their entirety and filed in central repositories in the custody of appropriate security officers or, in the case of the PCC combinations, to the Communications Programs Office according to distribution instructions printed on the card.

c. Domestically, the principal unit security officer will store the SF-700.

12 FAM 532.2-4 Storage of Combinations and Related Information

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. At a minimum, store combinations and related information in repositories authorized for the storage of material at the highest combined classification level to which combinations permit access. Except for the Security Container Information Card and cards posted inside repositories listing combinations in the immediate area, the recording of combinations is prohibited. Combinations must be committed to memory.

b. Combinations to repositories containing official funds are subject to the requirements of 4 FAM and the instructions of the responsible RSO. Money or other high-value items should not be collocated in a security container with classified information.

c. The names of personnel having knowledge of the combination must be posted on the inside of the control drawer of a safe file cabinet, on the inside of a vault door, or on the inside of the top drawer of a barlock cabinet using Form SF-700.

12 FAM 533 REMOVING CLASSIFIED MATERIAL FROM OFFICIAL PREMISES

12 FAM 533.1 Overnight Custody

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Classified material must not be removed from official premises except when necessary in the conduct of official meetings, conferences, or consultations and must be returned to safe storage facilities immediately upon the conclusion of the meeting, conference, or consultation. Residences are not considered official premises. Classified material must not be removed for reasons of personal convenience or be kept overnight in personal custody.

12 FAM 533.2 Certification Upon Permanent Departure from Post

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. When departing a post upon transfer, resignation, or retirement, each employee, irrespective of rank, must certify as part of the post clearance procedure that:

   (1) Classified material is not being taken from the post through other than authorized means;

   (2) Such material is not in their household or personal effects; and

   (3) Such material will not be mailed or otherwise transmitted in violation of 12 FAM 536.10.

b. Within A.I.D., provide certification on the SF-312 for employees and contractors with access to classified information. Contractors cleared for LOU will sign the AID-6-98, AID Separation Statement (see 12 FAM 533 Exhibit 533.2).

12 FAM 534 SAFEGUARDING CLASSIFIED MATERIAL

12 FAM 534.1 General Procedures

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Employees using classified material are responsible for its custody and must take every precaution to prevent deliberate or casual access to it by unauthorized persons.

b. Employees must not leave classified material in unoccupied rooms or inadequately protected in an occupied office, or in one occupied by individuals without security clearances and the need to know.

c. Cameras are not permitted in restricted areas or restricted buildings or in rooms containing classified material without prior approval from the Bureau of Diplomatic Security or regional security officer.

d. Foreign government information; employees must:

(1) Protect classified foreign government information and NATO information in the same manner as U.S. Government information of a comparable classification; and

(2) Safeguard foreign government and NATO RESTRICTED information as U.S. Government Confidential.

12 FAM 534.2 Closing Hours Security Check

12 FAM 534.2-1 SF-701, Activity Security Checklist

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Supervisors must institute a system of security checks prior to those conducted by security guards at the close of each working day, or as soon thereafter as administrative operations permit. Such a system ascertains that:

(1) All classified material, to include that processed on any automated information system, has been properly stored and that containers are locked;

(2) Windows and doors, where appropriate, are locked; and

(3) The area is otherwise secure and not susceptible to overt penetration.

b. In order to fulfill this fundamental mandatory requirement in all areas and

at all echelons, supervisory officials must designate employees on a weekly basis to conduct a closing hours security inspection of offices within a specifically defined area of responsibility. Such designees will use SF-701, Activity Security Checklist, to record the results of the closing hours security check. This form will be forwarded to the unit/post security officer (USO/PSO) at the end of the month. The USO/PSO will maintain the record for 30 days and then destroy it unless an incident has occurred which would warrant longer retention. Within A.I.D., forms SF-701 and SF-702 shall be filed for inspection purposes for a period of one year.

12 FAM 534.2-2 Reporting Infractions

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

An infraction of the regulations discovered by an employee designated to conduct the closing security check is not to be construed as a security violation in itself. It should not be reported on OF-117, Notice of a Security Violation (see 12 FAM 534 Exhibit 534.2-2), unless higher administrative authority determines otherwise or the closing hours security check is, in fact, the final inspection where U.S. citizen guards or Marine security guards are not on duty.

12 FAM 534.2-3 Responsibilities

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Employees designated to conduct closing hours security checks will, as a minimum:

   (1) Ensure that all repositories containing classified material are secured;

   (2) Ensure that all classified typewriter and printer ribbons, and laser printer cartridges are secured;

   (3) Check the tops of all desks, including “in” and “out” boxes, and repositories to ensure that all classified and controlled material has been put away; and

   (4) Make a visual check of the remainder of the office.

b. This section imposes a direct and important security responsibility on employees conducting closing hours checks. Although custodians of

classified material are responsible for its safekeeping in the Department and A.I.D., the checker, under certain circumstances, may be jointly charged with the violation.

12 FAM 534.2-4 Exceptions to Requirements

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Exceptions to the foregoing requirements, based upon physical or personnel considerations such as the unusual number of repositories located in a specific area, communications areas, alarmed rooms, and areas with few assigned employees, must be requested in writing to DS/CIS/IST or the RSO and will be decided on a case-by-case basis. Within A.I.D., forward exception requests to IG/SEC.

12 FAM 534.3 Conferences

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. In conducting conferences where classified information or material may be involved, the operations element calling or conducting the conference must observe every precaution to ensure that:

   (1) In the interests of technical security, classified conferences are held only on official premises;

   (2) Proper physical security measures are implemented to provide protection for such information or material equal to the measures required during normal operations; and

   (3) Participants are entitled to access to such information.

b. The operations element calling or conducting the conference should give advance notice to (and coordinate with) the appropriate post or RSO or DS/CIS/IST and within A.I.D., advance notice must be given to IG/SEC whenever:

   (1) Classified material is to be removed from its normal place of storage and transmitted or carried to the conference site; or

   (2) Participants are not personally known to have an appropriate security clearance by the officer calling or conducting the classified meetings.

12 FAM 535 ACCOUNTABILITY AND CONTROL

12 FAM 535.1 Control Procedures

12 FAM 535.1-1 General Requirements

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. E.O. 12356 requires the designation of Top Secret control officers (TSCOs) to provide positive control over the movement, use, and disposition of all Top Secret documents, to include those resident on automated information systems.

b. The use of a Top Secret Cover Sheet (SF-703) and a Top Secret Access Control Sheet (DS-1902) and a system of Top Secret control numbers and receipts are prescribed to ensure that Top Secret documents are fully accounted for at all times and that information is available on the identity of each person who has had access. (See 12 FAM 529 Exhibit 529.14-2 and 12 FAM 535 Exhibit 535.1-1.)

c. Top Secret information may not be placed on any ADP or WP system. It may be processed on an approved AIS (automated information system) or on a TEMPEST-approved typewriter.

d. Top Secret material which is also SCI, SAP, or COMSEC material must be accounted for and controlled by the procedures governing those programs. (See 12 FAM 660 regarding COMSEC.)

12 FAM 535.1-2 Designation of Top Secret Control Officers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. At each Foreign Service post, the principal officer will designate in writing a Top Secret control officer (TSCO) and an alternate to exercise control and maintain accountability records of material classified Top Secret (except COMSEC) in the custody of the post. The designated TSCO must be a senior officer at the post who can make the operational decisions concerning the use and distribution of the Top Secret material. The designated alternate is the communications programs officer due to the custody and storage requirements for Top Secret material. When the principal officer designates TSCOs and alternates, no action other than written notification to the regional security officer is required. The written notification should include the names and functional titles of the

designees and the date of designation.

b. Domestically, the executive director of each bureau or major organizational element will designate in writing a bureau TSCO and an alternate to exercise control and maintain accountability records of material classified Top Secret in the custody of the bureau. The designated bureau TSCO will be a senior grade officer of the bureau who can control the dissemination and storage of the material. Designated bureau TSCOs may, with the concurrence of DS/ISP/APB, designate unit TSCOs and alternates to aid them in the control and storage of Top Secret material in the various sections of the bureau, if operational necessity or physical locations require such additional designations. The bureau TSCO will have primary responsibility for the accountability of all material and records within the bureau, to include Top Secret information resident on automated information systems operated by a bureau or office. When bureau TSCOs and alternates are designated by the executive director, or unit TSCOs are designated by the bureau TSCO, the executive director or TSCO, as appropriate, sends a copy of the designation, including names, functional titles, area, room number, and telephone number to DS/ISP/APB and the principal USO.

c. In A.I.D., TDP, and OPIC, a central TSCO is located within the Office of the Executive Secretary. This central TSCO maintains lists of bureau TSCOs and coordinates and maintains the annual inventory.

12 FAM 535.1-3 TSCO Duties

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Maintain strict accountability over Top Secret material while under their jurisdiction.

b. Receive, store, issue, copy, and destroy all Top Secret material within their jurisdiction.

c. Maintain a permanent register to account for all Top Secret material either originated in or received in the area (using OF-116, Record of Top Secret Material). (See 12 FAM 535 Exhibit 535.1-3A for Form OF-116 and 12 FAM 535 Exhibit 535.1-1 for Form DS-1902, Top Secret Access Control Sheet.)

d. Maintain records of outgoing or destroyed Top Secret material on OF-112, Classified Material Receipt, or DS-1902, Top Secret Access Control Sheet, as appropriate, for five years. (See 12 FAM 535 Exhibit 535.1-1 and 12 FAM 535 Exhibit 535.1-3B.)

e. Review and change classification on Top Secret documents as directed by regulation or markings.

f. Destroy or arrange for retirement of Top Secret material as required by regulation or document markings.

g. Complete annual inventories using OF-123, Top Secret Document Inventory Record (see 12 FAM 535 Exhibit 535.1-3C) no later than October 31 and submit report to the cognizant RSO for posts and DS/ISP/APB for domestic offices. The RSO will notify DS/ISP/APB of any inventory discrepancies. In A.I.D., submit reports to the central TSCO with a copy to the Office of Security.

h. Assign appropriate Top Secret control numbers to Top Secret documents originating in or received within their area without a State control number. In A.I.D., the central TSCO assigns all control numbers.

i. Allow no copy of a Top Secret document to be made without the permission of the originating office/agency, unless specifically authorized in the document.

j. Ensure all Top Secret material is stored according to 12 FAM regulations.

k. Ensure that each individual who has access to the Top Secret document signs the Top Secret Access Control Sheet access section.

l. Review each Top Secret document during the inventory period with a view toward possible destruction, downgrading, declassification, or retirement of the document.

m. Ensure that no individual within their area of jurisdiction transmits Top Secret documents to another individual or section without the knowledge and consent of the TSCO and the completion of an OF-112.

n. Ensure compliance with automation security policies governing the control and protection of Top Secret information resident on automated information systems.

12 FAM 535.1-4 Inventories of Top Secret Documents

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. All TSCOs will conduct inventories of Top Secret documents upon change of custody and conduct an annual inventory to be completed as of October 31. An inventory conducted for change of custodian within two

months, either side, of October 31 will suffice for the annual inventory requirement. It is mandatory that the presence of each document be physically verified. Prepare the inventory on the Top Secret Document Inventory Record, OF-123. Immediately report any documents unreconciled at the time of the inventory to DS/ISP/APB. Domestically, forward a copy of the inventory to DS/ISP/APB no later than October 31. At post, the RSO will notify DS/ISP/APB of any inventory discrepancies. Within A.I.D., provide inventories and notification of problems to IG/SEC.

b. TSCOs will be held ultimately responsible for any loss of Top Secret documents under their jurisdiction which has been caused by improper administration of these requirements. If another individual of the area is directly responsible for the loss of any Top Secret material, that person will be held responsible for the loss of the information.

12 FAM 535.1-5 Administrative Action

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Any employee who loses Top Secret material, causes the compromise of Top Secret information or any portion thereof, makes a copy of a Top Secret document or any portion thereof without the TSCO's and originator's permission, or allows another employee who does not have a "need-to-know" to have access to Top Secret information is subject to administrative action as outlined in 3 FAM.

12 FAM 535.2 Secret and Confidential Control Procedures

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

There is no requirement for the specific control and accountability of either Secret or Confidential information.

12 FAM 536 ACCESS AND DISSEMINATION

12 FAM 536.1 General Access Requirements

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

No person may be given access to classified information unless that person has been determined to be trustworthy and unless such access is necessary in connection with the performance of official duties. Grant access to classified information in accordance with the criteria given in this section, and the person executes the SF-312, Nondisclosure Agreement Form.

12 FAM 536.1-1 Determination of Trustworthiness

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. No person shall be given access to classified information unless a favorable determination has been made as to the person's trustworthiness. The determination of trustworthiness, referred to as a security clearance, is based on such investigations as may be required in accordance with the applicable standards and criteria.

b. DS/ICI/PSS keeps a record of all security clearances for Department of State employees and contractors. IG/SEC keeps a record of security clearances for A.I.D. personnel. Special and specifically authorized clearances are required for access to information identified as Restricted Data, NATO, COSMIC, cryptographic, intelligence, and other information given special protection by law or regulation.

12 FAM 536.1-2 Determination of Need-to-Know

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

A person is not entitled to receive classified information solely by virtue of official position or by virtue of having been granted a security clearance. A person must also have a need for access to the particular classified information sought in connection with the performance of official U.S. Government duties or contractual obligations, or as otherwise specifically authorized by these regulations. The officers having responsibility for the classified information shall make the determination of that need.

12 FAM 536.1-3 Determination of Storage Capability

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

A person is not entitled to receive classified material solely by virtue of having a security clearance and a need to know. He or she must also have approved classified material storage facilities. Not all foreign affairs

agencies, or contractor facilities, domestically or abroad, have storage capability for classified material. Employees must contact the appropriate foreign affairs agency security office to verify storage capability.

12 FAM 536.1-4 Determination of Security Briefing

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

A person is not entitled to receive classified information until after he or she has received a security briefing covering the provisions of these regulations and has executed a non-disclosure agreement (Form SF-312) according to National Security Decision Directive 84 (NSDD 84) dated March 11, 1983.

12 FAM 536.2 Access by Historical Researchers and Former Presidential Appointees

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

As agency records for a particular period are declassified, they are transferred to the National Archives. Historical researchers, therefore, will normally be referred to the National Archives for research in such declassified records.

12 FAM 536.2-1 Department of State Records

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

For the Department, former Presidential appointees may apply to the Office of Freedom of Information, Privacy and Classification Review (A/IM/IS/FPC) for access to those documents which they originated, reviewed, signed, or received while serving as Presidential appointees, provided that all of the following conditions are satisfied:

(1) DS/ICI/PSS makes the determination that granting access to the intended recipient is consistent with the interests of national security and that the intended recipient is trustworthy. Access will be limited to categories of information over which the agency has classification jurisdiction;

(2) The intended recipient agrees in writing to safeguard the information from unauthorized disclosure in a manner consistent with applicable statutes and regulations;

(3) The intended recipient agrees in writing to authorize the review of notes and manuscripts for the purpose of determining that no classified information is contained therein;

(4) The intended recipient agrees in writing that the information involved will not be further disseminated without the express permission of the agency;

(5) The information requested is reasonably accessible and can be located and compiled with a reasonable amount of effort. Otherwise, A/IM/IS/FPC will charge fees to assemble the information, in accordance with the schedule in 22 CFR 171.6;

(6) Any individual or research assistant requiring access on behalf of the intended recipient must also meet all of the above conditions. Such personal assistants must be authorized to be working for the former appointee exclusively and not gathering information for publication on their own;

(7) Information compiled by research assistants is similarly subject to all conditions enumerated above; and

(8) Upon request, such information as the recipient may identify will be reviewed for declassification in accordance with the provisions of these regulations.

12 FAM 536.2-2 Other Agencies' Records

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. For A.I.D. and TDP, former Presidential appointees and historical researchers may apply to the Office of Public Affairs.

b. For OPIC, former Presidential appointees and historical researchers may apply to the Director of Legislative Affairs.

12 FAM 536.3 Access by Other Persons Outside the Executive Branch

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Provision of classified information to individuals or organizations of the Federal Government outside the Executive Branch will be determined on a

case-by-case basis by the Office of Freedom of Information, Privacy and Classification Review (A/IM/IS/FPC) in coordination with other concerned bureaus, including H and L; in OPIC by the Director of Public Affairs; and in A.I.D. by the Bureau for Legislative Affairs, Congressional Liaison Staff.

b. Subject to the above paragraph and 12 FAM 536.2 and 12 FAM 536.3, classified material will not normally be provided to persons outside the Executive Branch of the U.S. Government. However, exceptions may be made provided that all the conditions in 12 FAM 536.2 are satisfied.

12 FAM 536.4 Access by Contractors or Consultants

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. By agreement, the Secretary of Defense is authorized to act on behalf of the Department of State in rendering industrial security services. DS/ISP/INB will verify those contractor firms and personnel having current clearances to participate in classified contracts or purchase orders. For additional information refer to 12 FAM 230 and 12 FAM 570. Within A.I.D., IG/SEC conducts investigations and grants clearances to contractors.

b. Department employees are personally responsible for ensuring that DS/ISP/INB has authorized consultants and/or contractors to have access to classified information prior to release of any such information.

12 FAM 536.5 Access by Foreign National Employees

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Classified information must not be made available to, or left in the custody of, foreign national employees. Do not permit such employees to attend meetings where classified information is discussed.

b. Classified information must not be dictated to or typed by foreign national employees. This restriction must not be circumvented by the assignment of classification after such an employee has prepared a particular document. National Security information must not be entered into an automated information system (AIS) to which foreign nationals have access. The limitation against retroactively classifying data also applies

to any document prepared on an automated information system used by foreign nationals.

12 FAM 536.6 Controlling Official Dissemination

12 FAM 536.6-1 Other Federal Agencies

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Classified information that originated in another federal agency must not be communicated by the receiving agency to a third agency without the consent of the originating agency. For these purposes, State, OPIC, TDP, and A.I.D. are to be considered separate agencies. Such approval must be obtained in writing, and a record of the approval and communication must be maintained by the communicator.

b. Classified information may be sent to other federal agencies only through established liaison or distribution channels.

12 FAM 536.6-2 Dissemination Ordered or Requested by a Court of Law or Other Official Body

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Any subpoena, demand, or request for classified information or records from a court of law or other official body shall be handled in accordance with agency regulations (22 CFR Part 172; State, 5 FAM).

b. Testimony involving classified information is subject to the procedures for responding to subpoenas and must not be given before a court or other official body without the approval required by those procedures. An employee called upon to give such testimony without prior authorization shall state that to disclose the information desired is not authorized and that a written request for the specific information should be transmitted to the head of the agency concerned. Such testimony, when so approved, shall be given only under such conditions as the authorizing officer may prescribe.

c. All reports, records, and files relative to the loyalty of employees or prospective employees (including reports of investigative agencies) shall be maintained in confidence, and shall not be transmitted or disclosed except as required in the efficient conduct of business, and then only in accordance with applicable regulations.

12 FAM 536.6-3 Controls for Dissemination and Use of Intelligence Information

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Information contained in intelligence documents, including those produced by the Bureau of Intelligence and Research (INR), that is marked with specific control markings must be handled within the framework of the limitations imposed by such controls. For details and definitions of these controls, refer to 11 FAM. Failure to comply with these provisions will be considered a violation to be handled as prescribed under subchapter 12 FAM 550.

b. Information bearing the notation "WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating agency and an assessment by the senior intelligence official in the disseminating agency as to the potential risks to the national security and to the intelligence sources and methods involved.

c. In general, employees must clear with INR/DOC/OIL/CS telegrams and other documents originating in the Department of State which include or refer to classified intelligence information.

12 FAM 536.7 Disseminating U.S. Classified Information to Foreign Governments

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

For detailed instructions governing the release of classified information to foreign governments and international organizations, see 11 FAM.

12 FAM 536.7-1 Classified Military Information

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The National Disclosure Policy Committee (NDPC) establishes the procedures governing the release of classified military information to foreign governments and international organizations.

b. Direct all requests for the release of such information to:

National Military Information Disclosure Policy Committee (NDPC)
Director, Defense Trade Center
Bureau of Political-Military Affairs
U.S. Department of State
Washington, D.C. 20520

(See also 11 FAM.)

12 FAM 536.7-2 Crypto Marking

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

A designation or marking of "CRYPTO" applied to cryptographic material indicates that it requires special consideration with respect to access, storage, handling, and accounting. Contact the appropriate foreign affairs agency security office regarding these procedures. For the Department of State, contact Information Management's Cryptographic Systems Branch (A/IM/SO/TO/SI/CRYPT).

12 FAM 536.8 Personal Use and Conversations

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Classified information must not be used for personal interests of any employee and must not be entered in personal diaries or other non-official records.

b. Employees must not hold discussions of classified information in the presence or hearing of persons who are not authorized to have knowledge thereof.

c. Employees must not discuss classified information in conversations on nonsecure telephones or office intercoms.

12 FAM 536.9 Transmitting Classified Information

12 FAM 536.9-1 General Restrictions

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Under no circumstances will classified material be transmitted physically across international boundaries except by diplomatic courier or specially

authorized nonprofessional diplomatic couriers. Nonprofessional diplomatic couriers are given such material for international transporting only in emergencies, when the professional service will not cover the area into which the pouch must be carried or the post to which the pouch is addressed within the time that official business must be conducted. In such isolated cases, the nonprofessional diplomatic courier must be in possession of a diplomatic passport and a courier letter, and the material must be enclosed in sealed diplomatic pouches until delivered to its official destination. (See 12 FAM 100.)

b. See 12 FAM 536 Exhibit 536.9 for a guide on the transmission of classified and administratively controlled information.

12 FAM 536.9-2 Top Secret

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Top Secret information must be transmitted by either:

(1) Top Secret-cleared messenger;

(2) Authorized courier:

(a) Department of State Courier Service;

(b) Department of Defense Courier Service;

(c) Department of State nonprofessional courier; or

(3) Electrical means in encrypted form.

12 FAM 536.9-3 Secret and Confidential

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Secret and Confidential information may be transmitted via:

(1) One of the means approved for Top Secret;

(2) U.S. registered mail within and between the 50 States and the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession;

(3) U.S. Postal Service Express Mail. U.S. Postal Service Express Mail can 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 Mail label may not be executed under any circumstances. All classified express mail shipments shall be processed through mail distribution centers or delivered directly to a U.S. Postal Service facility or representative. The use of external (side street) express mail collection boxes is prohibited;

(4) U.S. registered mail facilities of the Army, Navy, Air Force, or other U.S. post offices outside the areas enumerated above, provided that the material does not at any time pass out of U.S. citizen employee control and does not pass through a foreign postal system.

12 FAM 536.9-4 Unclassified Material

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Unclassified material may be transmitted by diplomatic pouch, U.S. first-class mail, or through foreign postal systems according to instructions issued by principal officers. Unclassified information originating in the United States should go through the official communications center serving the agency of the sender.

12 FAM 536.9-5 Policy for Hand-Carrying Classified Documents

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Because of the security risk inherent in hand-carrying classified material, supervisors will authorize hand-carrying only when:

(1) The classified material is required at the destination;

(2) The classified material is not available at the destination; and

(3) Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

b. The classified material must be in the physical possession of the custodian at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (continental United States only) is available.

c. Classified material will not be brought home or to a hotel for storage prior to a trip.

d. Hand-carrying classified material on trips that involve overnight stopover is not permitted without advance arrangements for proper overnight storage at an approved Government activity.

e. Classified material may not be read, studied, displayed, or used in any manner on a public conveyance or in a public place.

f. Classified material is not to be stored in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank.

g. Whenever possible, return the classified material to the parent organization by one of the other approved methods of transmission.

h. For trips outside the continental United States, follow the requirements of 12 FAM 100 for designation as a nonprofessional courier.

12 FAM 536.10 Reproducing Classified Documents

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The number of copies of documents containing classified information must be kept to the minimum required by operational necessity to decrease the risk of compromise and reduce storage costs. All classified material shall be reproduced sparingly and any general or specific prohibition against reproduction shall be strictly adhered to. No classified document is to be reproduced if such reproduction is prohibited by the originator and the document is so annotated. Unauthorized reproduction of classified material will be subject to appropriate disciplinary action. Reproduced copies of classified documents are subject to the same accountability and controls as the original. However, these provisions shall not restrict the reproduction of documents for the purpose of facilitating review for declassification, but such reproduced documents that remain classified after review must be destroyed.

b. The TSCO of the reproducing office must obtain permission for reproduction of a Top Secret document unless otherwise marked from either the TSCO of the originating office or the TSCO of the operating element authorized to make initial distribution. Both the originating and reproducing offices must maintain appropriate records to reflect the number of copies reproduced and observe all other requirements concerning the control and distribution of such copies. In AID/W, the

Executive Secretary must approve the reproduction of Top Secret material unless otherwise marked, and only the ES staff can reproduce the material.

c. Unless a notation on the document or its cover restricts reproduction, permission is authorized without the approval of the originating department or agency for the reproduction of Secret and Confidential documents. Reproduction of the documents must be limited to that which is essential for efficient operations.

d. All agencies that reproduce paper copies of classified documents shall maintain records to show the number and distribution of reproduced copies:

(1) Of all Top Secret documents;

(2) Of all documents covered by special access programs distributed outside the originating agency;

(3) Those distributed within the agency if required by the special access program; and

(4) Of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations.

e. Also, when reproduction beyond the initial production is required, the copy from which reproduction is made must show the authority for reproduction, the officer requesting reproduction, and the number of copies made.

f. Classified material should only be reproduced on those reproduction machines under the continuous control of cleared U.S. personnel.

12 FAM 537 DISPOSITION OR DESTRUCTION

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Classified material must be carefully and completely destroyed only through authorized means by cleared U.S. citizen employees. See 12 FAH-1, *Emergency Planning Handbook*, regarding emergency destruction of materials.

12 FAM 538 SPECIAL ACCESS PROGRAMS

(SAPS)

12 FAM 538.1 Policy

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

See section 4.2 of E.O. 12356 regarding special access programs. Special access programs may be created or continued only under specific circumstances showing that:

(1) Normal management and safeguarding procedures are not sufficient to limit "need-to-know" or access; and

(2) The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

12 FAM 538.2 Control and Administration

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Each office shall appoint an official to act as a single point of contact for information concerning the establishment and security administration of all SAPs established by or existing in the office.

12 FAM 538.3 Codewords and Nicknames

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Excluding those programs specified in 12 FAM 539.6-1, paragraphs a and b, each SAP will be assigned a codeword, a nickname, or both. Only the Assistant Secretary for Diplomatic Security through the official appointed under 12 FAM 539.6-2 shall allocate codewords and nicknames for SAPs. All codewords and nicknames are unclassified. Within A.I.D., the Executive Secretary (ES) will assign codewords and nicknames.

12 FAM 538.4 Reporting Requirements

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Excluding those programs specified in 12 FAM 539.6-1, paragraphs a and b, offices administering SAPs provide annual reports (Report number F-92-1) to the Assistant Secretary for Diplomatic Security, submitting them not later than January 31 of each year, showing the changes in information provided under 12 FAM 539.6-1, as well as the date of last review. Annual reports shall reflect actual rather than estimated numbers of carve-out contracts and persons granted access and shall summarize the results of the inspections and audits required by 12 FAM 539.6-2, paragraph a. The information in the annual report shall be as of December 31. Within A.I.D., this will be accomplished by the Executive Secretary (ES).

b. Administering offices must immediately notify DS/ISP/APB upon termination of a SAP. Within A.I.D., notify the Executive Secretary (ES).

12 FAM 538.5 Limitations on Access

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Access to data reported under this section shall be limited to the minimum number of properly indoctrinated staff necessary to perform the functions assigned to DS/ISP/APB for the Department of State. Access may not be granted to any other person for any purpose without the approval of the office sponsoring the SAPs concerned.

12 FAM 538.6 "Carve-Out" Contracts

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The official charged with the program and the Assistant Secretary for Diplomatic Security, or their designees, shall ensure that, in those SAPs involving contractors, special access controls are made applicable by legally binding instruments. (See 12 FAM 570.) Within A.I.D., this will be accomplished by IG/SEC.

b. Excluding those programs which are specified in 12 FAM 539.6-1, paragraphs a and b, the use of "carve-out" contracts that relieve the Defense Investigative Service from inspection responsibility under the Industrial Security Program is prohibited unless:

(1) Such contract supports a SAP approved and administered under 12 FAM 539.6-1;

(2) Mere knowledge of the existence of a contract or of its affiliation with the SAP is classified information; and

(3) DS/ISP/APB approves carve-out status for each Department of State contract.

c. Approval to establish a "carve-out" contract must be requested from DS/ISP/APB. Within A.I.D., this will be accomplished by IG/SEC. Offices managing approved "carve-out" contracts must ensure the support necessary for the requisite protection of the classified information involved.

d. An annual inventory of carve-out contracts shall be conducted by each office which participates in SAPs.

e. This section relates back to the date of execution for each contract to which carve-out contracting techniques are applied. The carve-out status of any contract expires upon termination of the SAP which it supports.

12 FAM 539 PROCEDURES FOR STORING AND SAFEGUARDING CLASSIFIED INFORMATION

12 FAM 539.1 Precautions

(TL:DS-81; 01-31-2002)
(Uniform State, AID, OPIC, TDP)

a. Holders must use Open/Closed signs on every repository containing classified material to indicate that the container is either open or locked. The cognizant foreign affairs agency security officer can provide information regarding procurement of these signs.

b. All personnel handling classified and administratively controlled material are responsible for placing a cover sheet on the material to prevent unauthorized access and to alert personnel of the requirement for proper storage. Forms SF-703, *Top Secret Cover Sheet*, SF-704, *Secret Cover Sheet*, and SF-705, *Confidential Cover Sheet*, are the only authorized cover sheets for classified information.

c. Holders must affix a Security Container Check Sheet, SF-702, (see 12 FAM 539 Exhibit 539.1A) to every repository containing classified material and employees opening or closing the container must complete the appropriate column. (Any person opening a container is responsible for securing it, or obtaining explicit concurrence from another employee that

they will secure it.)

d. Holders must affix an Activity Security Checklist, SF-701, (see 12 FAM 539 Exhibit 539.1B) adjacent to at least the main exit door of every office where classified material is stored. This form is to be initialed at the end of the day by either the assigned security checker of the day or the last person to leave the office.

e. Personnel must ensure that classified repositories are locked and should check and initial those repositories that had not been opened since the previous check prior to leaving the room unattended. When securing a combination lock, turn the dial at least four complete turns in the same direction after closing. At the end of the day, the security checker is to check the lock and initial the SF-702, certifying that the lock has been secured by attempting to open the lock, drawers, or door. Anyone remaining after normal working hours is responsible for securing and checking their own safe.

f. Employees must immediately report defects or malfunctioning of storage equipment or locking devices to the unit security officer or the post security officer. Uncleared personnel are not permitted to service any equipment to be used for the storage of classified material.

g. Before taking security containers out of use, custodians must thoroughly inspect them to ensure all classified material has been removed and a standard combination set. The unit security officer and the property accountable officer will also inspect the property, and all will sign the Form OF-302, Excess Property Inspection Certification (see 12 FAM 539 Exhibit 539.1C). When checking safes that contain drawers, custodians must remove the drawers, and completely inspect the inside of the safe. When containers are moved from inactive to active service, custodians must inspect the container and locks for possible tampering.

h. Classified material must not be stored in desks or anywhere other than in approved storage containers.

i. Classified material, including disposable material such as rough drafts, shorthand notes, extra carbon or tissue copies, used carbon paper, hectograph masters, mimeograph stencils, typewriter or printer ribbons, disk drives, removable media from TEMPEST- approved systems, laser printer cartridges, and voice recording materials must be safeguarded and locked in appropriate security repositories whenever unattended. Unclassified typewriter ribbons and voice recording materials should be safeguarded and locked in appropriate security repositories at the close of business. This is a sound security practice and is advantageous to efficient administrative operations. For these same reasons, a ”clean

desk" policy of securing all classified and unclassified documents is strongly encouraged.

j. All keys to doors kept locked after working hours must be turned in to a U.S. citizen guard force and released only to authorized personnel. Where no U.S. citizen guard force is assigned, DS/CIS/IST or the RSO may authorize personal custody of keys. Keep such instances to an absolute minimum. Domestically, doors will be secured by means of a DS/CIS/DO-approved lock. DS/CIS/IST or the cognizant RSO must approve beforehand all new door lock installations. Desks, bookcases, and credenzas are not permitted to be locked either domestically or at post. For A.I.D., IG/SEC personnel will approve locks, lock installations, and personal retention of keys.

12 FAM 539.2 Top Secret Control Numbers

12 FAM 539.2-1 Required Assignment of Top Secret Control Numbers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Top Secret control officers (TSCOs) must mark a Top Secret control number at the top right-hand front of each copy of each Top Secret document when originated or received. TSCOs must destroy draft copies when a final version is produced and distributed. If it is necessary to retain a draft copy because of draft clearances or for other reasons, TSCOs must assign it the original series designation control number and a copy number.

b. TSCOs must also place Top Secret control numbers on forms required for the control of Top Secret information, such as Top Secret Access Control Sheet, DS-1902; Top Secret Document Inventory Record, OF-123; and Record of Top Secret Material, OF-116.

12 FAM 539.2-2 Composition of Top Secret Control Numbers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. A Top Secret control symbol belongs to the post or organizational element. Each successive TSCO shall use the same post or organizational element symbol. Control symbols are given in 12 FAM 539 Exhibit 539.2-

2.

b. The Top Secret control number consists of the control symbol of the organization element, the last two digits of the calendar year, the consecutive number of the Top Secret document originated or received that year, and the copy number. For example:

(1) If the Top Secret control number is LND-89/17, copy 3, LND is the Top Secret control symbol for London; 89 indicates the calendar year; 17 indicates the 17th Top Secret document either originated or received at post that year; and copy 3 indicates the third copy made of LND-89/17; or

(2) If the Top Secret control number is EUR-89/37, copy 5, EUR is the Top Secret control symbol for the Bureau of European and Canadian Affairs; 89 indicates the calendar year; 37 indicates the 37th Top Secret document either originated or received in EUR that year; and copy 5 indicates the fifth copy made of EUR-89/37.

12 FAM 539.2-3 Assigning Top Secret Control Numbers

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Upon the origination of a Top Secret document, or the receipt of one without a Top Secret control number, the TSCO must immediately:

(1) Assign a post or organizational element Top Secret control number;

(2) Place it on the document; and

(3) Affix a completed Top Secret Access Control Sheet and a Top Secret Cover Sheet to each document.

b. See 12 FAM 539 Exhibit 539.2-3 regarding reproduced Top Secret Documents.

c. In A.I.D., these functions are reserved solely to the central TSCO.

12 FAM 539.2-4 Top Secret Cover Sheets

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. The original and each copy of Top Secret documents must be covered by a Top Secret Cover Sheet and a Top Secret Access Control Sheet. The

TSCO must complete the DS-1902 and include the control number, the type of material, subject matter, date, addressee, and originator. All persons having access to the document attached to the Top Secret Cover Sheet and the Top Secret Access Control Sheet must sign and date the access control sheet before accepting responsibility for its custody. The Top Secret Access Control Sheet must remain with the document until the document is:

(1) Transferred to another agency;

(2) Destroyed;

(3) Retired;

(4) Downgraded; or

(5) Declassified.

b. When one of the above listed actions is taken, the TSCO must record the action on the Top Secret Access Control Sheet, retain it in the files for five years, and then destroy it.

12 FAM 539.2-5 Distribution

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Top Secret documents distributed outside the area of the TSCO must be accompanied by either a Classified Material Receipt, OF-112, or Receipt Manifest, DS-794 (see 12 FAM 539 Exhibit 539.2-5), in duplicate. For accountability purposes, receipts reflecting the transmission of Top Secret material must be filed separately from receipts concerned with material of lesser classification. (See also 12 FAM 539.4-2.)

b. TSCOs or designated alternates are responsible for the accountability, proper handling, and storage of Top Secret material. Top Secret material cannot be left in MDLs even during operational hours of the PCC. Distribution of Top Secret documents will be made only by the TSCO or alternate. All persons who read or who have access to a Top Secret document must sign their names and date on the reverse of the Top Secret Cover Sheet. No individual responsible for a Top Secret document may transmit it to another individual or section without the knowledge and consent of the TSCO.

c. Direct receipt of Top Secret documents from outside the area by an employee other than the TSCO must be immediately turned over to the

TSCO for appropriate accountability. No employee other than the TSCO will transfer Top Secret documents out of the area of jurisdiction.

12 FAM 539.3 Authorized Special Distribution Captions

(TL:DS-67; 05-22-2000)
(Uniform State, AID, OPIC, TDP)

a. **NO DISTRIBUTION (NODIS)** means no distribution to other than addressee without the approval of the Executive Secretary. This caption is used only on messages of the highest sensitivity between the President, the Secretary of State, and chiefs of mission. Documents bearing this special distribution caption shall be treated as NOFORN. These documents must be given the physical protection prescribed by their classification. See 5 FAH-4 H-213.1 for additional guidance.

b. **EXCLUSIVE DISTRIBUTION (EXDIS)** means distribution exclusively to officers with essential need-to-know. This caption is used only for highly sensitive traffic between the White House, the Secretary, the Under Secretaries, and chiefs of mission. Documents bearing this special distribution caption shall be treated as NOFORN. These documents must be given the physical protection prescribed by their classification. See 5 FAH-4 H-213.1 for additional guidance.

c. **LIMITED DISTRIBUTION (LIMDIS)** means distribution strictly limited to officers, offices, and agencies with need-to-know. This caption is reserved for messages of more than usual sensitivity. Material captioned "LIMDIS" is to be controlled, handled, and stored in accordance with the classification level of the information involved.

d. **STATE DISTRIBUTION only (STADIS)** precludes initial distribution to other federal agencies and is used when disclosure of certain communications to other agencies would be prejudicial to the best interests of the Department of State. This caption may be used in conjunction with the captions "EXDIS" and "LIMDIS." Material captioned "STADIS" is to be controlled, handled, and stored in accordance with the classification level of the information involved

e. For details regarding caption messages, see 5 FAM.

12 FAM 539.4 Procedures for Access and Dissemination

12 FAM 539.4-1 Covers and Envelopes

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Except as noted below, all classified materials must be double-wrapped in opaque envelopes or paper.

b. Classified documents must be covered by a cover sheet or folded inwards and be enclosed in an opaque envelope. Material transmitted via pouch (i.e., by diplomatic courier), by authorized messenger, or by pneumatic tube (within the Department's headquarters (Main State) building) need not be enclosed in a second or outer envelope because the pouch, the messenger's portfolio, or the pneumatic tube carrier are considered second or outer covers.

c. Address the inner envelope to the appropriate official by name, title, and post/organization. It must be marked conspicuously on both sides with the appropriate classification, and contain a return address.

d. Employees must address the required outer envelope for U.S. mail in the same manner, but without a security classification or any other indication that the contents are classified. The envelope must also contain a return address, but will not contain a person's name.

e. If the package is destined for a post abroad and is being sent from outside Department channels but via diplomatic courier, employees must address the outer envelope to:

   U.S. Department of State
   Chief, Mail and Pouch Facility
   Washington, D.C. 20520-0258

   Employees must address the inner envelope as indicated above.

f. For posts or for Department of State contractor facilities, safeguarding capability can be verified through DS/ISP/INB. (See 12 FAM 536.1-3.)

12 FAM 539.4-2 Receipts and Registration

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Employees must use a Classified Material Receipt, OF-112, Receipt Manifest, DS-794 (see 12 FAM 535 Exhibit 535.1-3A and 12 FAM 539 Exhibit 539.2-5), or other receipt approved by foreign affairs agency security offices for Top Secret and Secret material transmitted outside the

organizational control of the sender. These receipts may be used for the transmission control of any other material at the discretion of the sender.

b. Employees must prepare OF-112, Classified Material Receipt, so that all items are completed and signatures are recorded on parts I, III, and IV. The unit maintaining records of receipt must retain these parts, together with part V, for two years. If all the items identified in Part IV are not received, the addressee or unit maintaining records of receipt will promptly notify the sender. If Part IV is not promptly returned to the sender or unit maintaining records of transmission, the unit maintaining records of receipt must notify the addressee. In either case should the error not be resolved, the sender shall notify security personnel (foreign affairs agency security offices or the RSO). The identity of enclosures (on parts I, IV, and V) shall include the type of document, subject, copy number and series, and date of document. Several items may be transmitted to the same address under cover of a single OF-112, provided a listing of the items is retained by the sender and a copy accompanies part V for the addressee's use. Instructions for the preparation and disposition of the OF-112 are contained on it. For all classified mail leaving the organizational unit of the sender, the sender maintains a record of the registration number, or Part V number, for two years. (NOTE: Classified titles are not to be used on the OF-112.)

c. Employees must use Form DS-794, Receipt Manifest, or other approved receipt, to cover the transmission of more than one classified document between the sender and a single addressee. Such receipts are forwarded in duplicate, so that the addressee may acknowledge receipt of the material by signing and returning a copy to the transmitter, retaining the original for addressee's records. The unit maintaining records of receipt must retain such receipts for two years.

d. Except as provided for the control of Top Secret material, originating and receiving elements or employees are not required to maintain additional logs of transmission and receipt of classified material other than to note internal distribution, which may be recorded on part V of the OF-112, the original of DS-794, or other approved means. Two years after the date of transmission or receipt of classified material, receipts covering the transaction may be destroyed.

e. Each piece (envelope, package, or other outer cover) of classified material going through the Diplomatic Pouch must be registered by the use of an OF-120, Diplomatic Pouch Mail Registration (see 12 FAM 539 Exhibit 539.4-2).

12 FAM 539.5 Procedures for Destruction

12 FAM 539.5-1 Destruction of Top Secret Material

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Top Secret control officers (TSCOs) are required to record destruction of Top Secret material on the corresponding Top Secret Access Control Sheet and retain the control sheet for five years after date of destruction.

b. The Top Secret control officer in recording the destruction of a Top Secret document must sign Form DS-1902 as the officer destroying the document, and one other Top Secret cleared U.S. citizen employee must sign as witness to the actual destruction; or, they must sign as participants in preparing the material for destruction, i.e., tearing and depositing in burn bags and securing the burn bags for destruction.

12 FAM 539.5-2 Destruction of Secret and Confidential Material

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

Records of destruction need not be made for Secret or Confidential material unless recording is required by special regulation. Employees must record destruction on Register - Destruction of Classified Material, JF-58 (see 12 FAM 539 Exhibit 539.5-2), or other form or log approved by the cognizant foreign affairs agency security office or the RSO. Information subject to special regulations such as NATO, Restricted Data, etc., must be destroyed and destruction recorded in accordance with requirements of the applicable regulation.

12 FAM 539.5-3 Using Burn Bags

(TL:DS-64; 01-03-2000)
(Uniform State, AID, OPIC, TDP)

All classified material, to include working papers, handwritten notes, word processing multistrike ribbon containers, and typewriter ribbon cartridges, to be destroyed must be placed in containers designated as burn bags, which are clearly and distinctly recognizable as burn bags. Burn bags awaiting destruction must be protected by safeguards commensurate with the classification designation of the material involved.

12 FAM 539.5-4 Laser Toner Cartridges

(TL:DS-64; 01-03-2000)
(Uniform State, AID, OPIC, TDP)

Laser toner cartridges removed from equipment such as laser printers, facsimile machines, and copiers may be treated, handled, stored, and disposed of as UNCLASSIFIED without additional countermeasures after completing a print cycle. When a cartridge is removed prior to completing a print cycle, handle as UNCLASSIFIED after manually rotating the drum one full turn.

12 FAM 539.5-5 Destruction Methods

(TL:DS-64; 01-03-2000)
(Uniform State, AID, OPIC, TDP)

Classified material is normally destroyed by burning, shredding, or, with the exception of microforms, by disintegration. DS/CIS/IST maintains a list of approved destruction equipment. Any other method must have the approval of the cognizant foreign affairs agency security office. Destruction of classified microforms can only be accomplished by burning or by chemical means, i.e., immersion in an approved chemical solution for a specified period of time, in accordance with Department instructions. COMSEC material must be destroyed in accordance with S-KAG. Within A.I.D., IG/SEC will maintain a list of approved destruction equipment and will approve alternate methods.

12 FAM 539.5-6 Destruction of Classified Removable Magnetic Storage Media

(TL:DS-64; 01-03-2000)
(Uniform State, AID, OPIC, TDP)

All removable magnetic data and program storage media which have been used for processing classified data must be destroyed in accordance with established guidelines for the destruction of this media. For the Department of State, employees must contact DS/ISP/SSB regarding these guidelines. For other foreign affairs agencies, their employees must contact the cognizant security office for further information.

12 FAM 539.6 Procedures for Special Access Programs

12 FAM 539.6-1 Establishing a Special Access Program

(TL:DS-61; 10-01-1999)
(Uniform State, AID, OPIC, TDP)

a. Procedures for the establishment of SAPs involving NATO classified information are based on international treaty requirements.

b. SAPs for foreign intelligence information under the cognizance of the Director of Central Intelligence (DCI), or those of the National Telecommunications and Information Systems Security Committee, originate outside the foreign affairs agencies and are subject to the directives and regulations of the DCI.

c. Excluding those programs specified in paragraphs a and b of this section, SAPs shall be established within the foreign affairs agencies by submitting to the agency head a complete justification which is to include:

(1) The rationale for establishing the SAP, including the reason why normal management and safeguarding procedures for classified information are inadequate;

(2) The estimated number of persons to be granted special access in the responsible component, other components, other U.S. Government agencies, contractors, and the total of such personnel;

(3) A summary statement pertaining to the program security requirements, with particular emphasis upon those personnel security requirements governing access to program information;

(4) The relationship, if any, to other SAPs in the Department or other U.S. Government agencies;

(5) The estimated number and approximate dollar value, if known, of carve-out contracts (see 12 FAM 538.6) that will be or are required to support the program;

(6) The component official who is the point of contact (last name, first name, middle initial, their position or title, mailing address, and telephone number);

(7) The proposed codeword and/or nickname (see 12 FAM 538.3) of the program; and

(8) The proposed date of program establishment.

12 FAM 539.6-2 Reviews of Special Access Programs

(TL:DS-61; 10-01-1999)

(Uniform State, AID, OPIC, TDP)

a. DS/ISP/APB shall be provided and will maintain a listing of all SAPs within the Department. INR/EX/SB will compile and maintain the list for all DCI SAPs in State and A.I.D. Within A.I.D. (except DCI SAPs), the Executive Secretary (ES) will maintain this list.

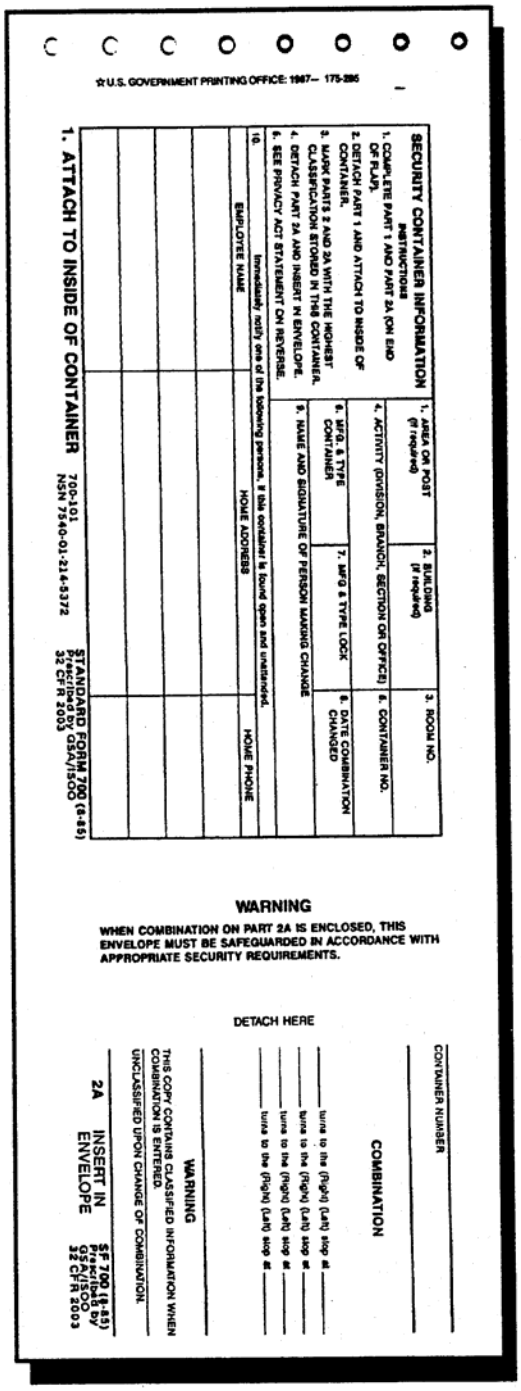
b. DS/ISP/APB shall conduct oversight reviews, as required, to determine compliance with this procedure and the general safeguarding of classified information. For DCI SAPs in State and A.I.D., INR/EX/SB will be the primary security office for oversight reviews. As necessary, INR/EX/SB and DS/ISP/APB will coordinate for assistance/support. Within A.I.D. (except DCI SAPs), IG/SEC will conduct these reviews.

c. Excluding those programs specified in 12 FAM 539.6-1, paragraphs a and b, the office administering each SAP shall review the program annually. To accommodate such reviews, the responsible office shall institute procedures to ensure the conduct of annual security inspections and regularly scheduled audits.

d. SAPs, excluding those specified in 12 FAM 539.6-1, paragraphs a and b, or those required by treaty or international agreement, shall terminate automatically every 5 years unless reestablished in accordance with the procedures contained in 12 FAM 539.6- 1, paragraph c.

12 FAM 532 EXHIBIT 532.2-3 SF-700, SECURITY CONTAINER INFORMATION FORM

(TL:DS-61; 10-01-1999)



SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

☆U.S. GOVERNMENT PRINTING OFFICE: 1987— 175-285

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

2A INSERT IN ENVELOPE

SF 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.
UNCLASSIFIED UPON CHANGE OF COMBINATION.

CONTAINER NUMBER _____

COMBINATION

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

12 FAM 534 EXHIBIT 534.2-2 OF-117, NOTICE OF A SECURITY VIOLATION

(TL:DS-61; 10-01-1999)

OPTIONAL FORM 117
March 1994 —STATE—AID—USIA
50117-103

NOTICE OF A SECURITY VIOLATION

BLDG. OR POST	
ROOM	OFFICE OCCUPYING ROOM

VIOLATION

NATURE OF VIOLATION	DATE	TIME

DISPOSITION TAKEN BY GUARD *(Including persons notified)*

COMMENTS

REGULATION REFERENCE	SIGNATURE OF GUARD

12 FAM 535 EXHIBIT 535.1-1 DS-1902, TOP SECRET ACCESS CONTROL SHEET

(TL:DS-61; 10-01-1999)

UNITED STATES DEPARTMENT OF STATE

ACCESS CONTROL SHEET

TOP SECRET

INFORMATION

TOP SECRET CONTROL NUMBER

DESCRIPTION

TELEGRAM, MEMO, LETTER, ETC.

SUBJECT/TITLE (UNCLASSIFIED)

ORIGINATOR | DATE

ADDRESSEE

COPY INFORMATION

☐ ACTION COPY ☐ INFORMATION COPY | COPY NO. _____ OF _____ COPIES.

TOP SECRET CONTROL OFFICER'S SIGNATURE | OFFICE SYMBOL | DATE

EACH PERSON WHO RECEIVES THIS DOCUMENT SHALL PRINT THEIR NAME, ORGANIZATION SYMBOL AND DATE IN THE SPACES PROVIDED ON THE REVERSE OF THIS FORM

TOP SECRET ATTACHMENTS, IF ANY, SHALL BE LISTED ON THIS CONTROL SHEET AND ANNOTATED WITH THE COVER DOCUMENT CONTROL NUMBER.

THIS CONTROL SHEET SHALL NOT BE REMOVED UNTIL THE TOP SECRET DOCUMENT IT CONTROLS IS TRANSFERRED OUTSIDE OF STATE, OR DOWNGRADED, DECLASSIFIED, DESTROYED, OR RETIRED. THE TOP SECRET CONTROL OFFICER TAKING THE ACTION SHALL SIGN HIS/HER NAME, ORGANIZATION SYMBOL AND DATE AND NOTATE THE ACTION. THE OFFICER SHALL FILE THIS TOP SECRET CONTROL SHEET IN HIS/HER FILES, RETAIN IT FOR FIVE YEARS, AND THEN DESTROY THE SHEET.

☐ TRANSFERRED	ADDRESSEE	OF-112 SERIAL NO.
☐ DOWNGRADED OR DECLASSIFIED	DATE	NEW CLASSIFICATION
☐ DESTROYED ☐ RETIRED	DATE	SIGNATURE OF WITNESS
TOP SECRET CONTROL OFFICER'S SIGNATURE		DATE
TYPED NAME AND ORGANIZATIONAL SYMBOL OF TOP SECRET CONTROL OFFICER		

FORM 10-92 DS-1902

TOP SECRET ACCESS RECORD

NAME	OFFICE SYMBOL	DATE

TOP SECRET

12 FAM 535 EXHIBIT 535.1-3A FORM OF-116, RECORD OF TOP SECRET MATERIAL

(TL:DS-61; 10-01-1999)

RECORD OF TOP SECRET MATERIAL

1	2			3	4	5	6	7	8
COVER SHEET NUMBER	Check (✓) Indicate Copy No.			DATE RECEIVED	RECEIPT NUMBER (OF-112)	DESCRIPTION	DISTRIBUTION (Office Symbol)	SIGNATURE (Control Officer)	FINAL DISPOSITION
	Action	Info.	Copy No.						

50116-102

OPTONAL FORM 116 (formerly Form JF-10)
November 1978-STATE-AID-USIA

12 FAM 535 EXHIBIT 535.1-3B OF-112, CLASSIFIED MATERIAL RECEIPT

(TL:DS-61; 10-01-1999)

☆ U. S. GOVERNMENT PRINTING OFFICE: 1985—481-128

DATE SENT: _____ **Classified Material Receipt** V 2623070

FROM: _____
(Name) (Office Symbol) (Room No.) (Bldg.)

TO: _____
(Name) (Office Symbol) (Room No.) (Bldg.)

PART I

_____
(Messenger's Signature)

IDENTIFICATION _____

_____

_____

Optional Form 112
Rev. 8/79
State AID USICA
50112–102

THIS PART IS TO BE FILLED IN AND RETAINED BY SENDER UNTIL RETURN OF PART IV AND ATTACHED THERETO

(Office symbol or Stamp with Date and Hour)

THIS PART TO REMAIN ATTACHED TO PART II BUT NOT FIXED TO ENVELOPE
TO BE SIGNED BY RECIPIENT AND RETURNED BY MESSENGER TO CENTRAL MESSENGER UNIT
RETAINED FOR 3 YEARS

V

12 FAM 535 EXHIBIT 535.1-3C FORM OF-123, TOP SECRET DOCUMENT INVENTORY RECORD

(TL:DS-61; 10-01-1999)

TOP SECRET DOCUMENT INVENTORY RECORD

OFFICE OR POST

AS OF OCTOBER 31, 19

SUBMITTED BY (Signature of Top Secret Control Officer)

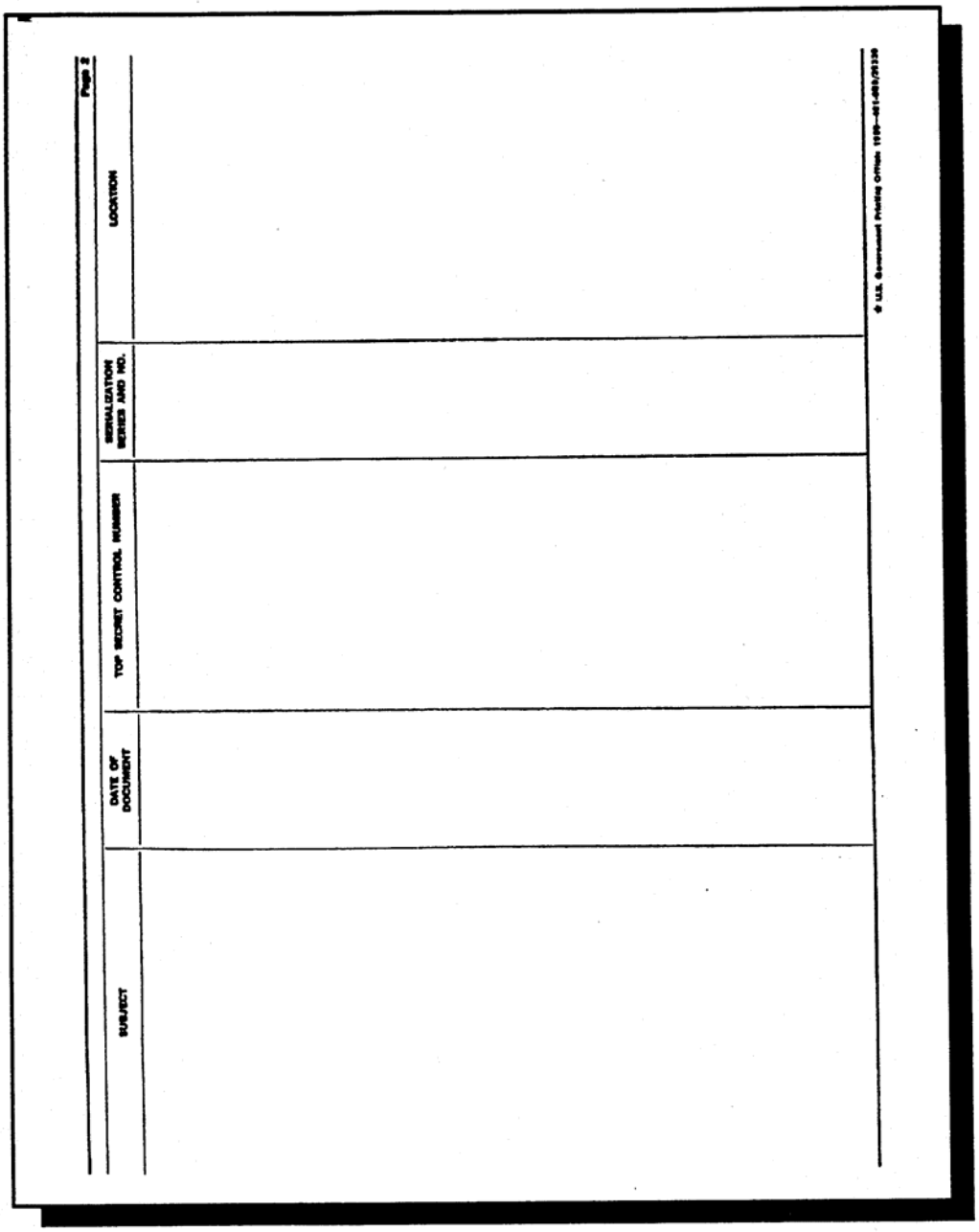
Typed Name:

SUBJECT	DATE OF DOCUMENT	TOP SECRET CONTROL NUMBER	SERIALIZATION SERIES AND NO.	LOCATION

50123-101

(over)

OPTIONAL FORM 123 (Formerly Form JF-17)
AUTHORITY: 5 FAM 1
STANDARD—AID—USIA



SUBJECT	DATE OF DOCUMENT	TOP SECRET CONTROL NUMBER	SERIALIZATION SERIES AND NO.	LOCATION

Page 2

☆ U.S. Government Printing Office: 1989—401-003/20330

12 FAM 539 EXHIBIT 539.1A FORM SF-702, SECURITY CONTAINER CHECK SHEET

(TL:DS-61; 10-01-1999)

SECURITY CONTAINER CHECK SHEET

TO (if required) | THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

702-101
NSN 7540-01-213-7900

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

SECURITY CONTAINER CHECK SHEET

TO (If required) | THRU (If required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

702-101
NSN 7540-01-213-7900

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

12 FAM 539 EXHIBIT 539.1B FORM SF-701, ACTIVITY SECURITY CHECKLIST

(TL:DS-61; 10-01-1999)

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(if required)* FROM *(if required)* THROUGH *(if required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

12 FAM 539 EXHIBIT 539.1C OF-302, EXCESS PROPERTY INSPECTION CERTIFICATION

(TL:DS-61; 10-01-1999)

OPTIONAL FORM 302(1-85)
DEPT. OF STATE

EXCESS PROPERTY INSPECTION CERTIFICATION

Inspection of excess property must be made prior to release as excess or transfer. For ADP equipment, appropriate degaussing/sanitizing measures must take place before removal. Check the appropriate box below to indicate the type of property involved and certify by appropriate personnel. Affix the certification to each property item with drawers and/or shelves, and to typewriters, word processors, and other ADP equipment.

☐ FURNITURE/SAFE/CABINET	☐ MACHINE/SYSTEMS EQUIPMENT	
☐ Drawers/shelves inspected and determined clear of any content	BRAND NAME	MODEL NO.
	SERIAL NO.	
☐ Combination reset to 50–25–50 (safe)	☐ RIBBON REMOVED OR STORAGE MEDIA CLEARED	

INSPECTION CERTIFICATION

FROM (OFFICE)	PROPERTY ACCOUNTABLE OFFICER
CUSTODIAN/OPERATOR NAME (PRINT)	NAME (PRINT)
SIGNATURE	SIGNATURE
RECEIVED BY	UNIT SECURITY/ INFORMATION SYSTEMS OFFICER
NAME (PRINT)	NAME (PRINT)
SIGNATURE	
TITLE	SIGNATURE
ORGANIZATION / DATE	

NSN 7540-01-197-0221 50302-101

12 FAM 539 EXHIBIT 539.2-2 TOP SECRET CONTROL SYMBOLS ASSIGNED TO FOREIGN SERVICE POSTS

(TL:DS-61; 10-01-1999)

This listing does not reflect active/inactive status of any post. Consult 2 FAM for this information.

Post	**Symbol**
A	
Abidjan	ABJ
Abu Dhabi	ABD
Accra	ACC
Adana	ADA
Addis Ababa	ADD
Adelaide	ADL
Aden	ADN
Alexandria	ALX
Algiers	ALG
Amman	AMS
Ankara	NK
Antananarivo	ANT
Antwerp	ATW
Asmara	ASM
Asuncion	ASN
Athens	ATH

Auckland	ACK
B	
Baghdad	ACK
Baida	BDA
Bamako	BAM
Bangui	BAM
Banjul	BAM
Barcelona	BAN
Barranquilla	BRC
Beijing	BRR
Beirut	BRT
Belem	BLM
Belfast	BLF
Belgrade	BLG
Belize City	BLZ
Benghazi	BLZ
Berlin (East)	BFP
Berlin (West)	BRL
Bern	BEN
Bilbao	BIS
Bogota	BGT
Bombay	BMB
Bonn	BNN
Bordeaux	BRD

Brasilia	BRA
Brazzaville	BRZ
Bremen	BRN
Bridgetown	BRN
Brisbane	BRN
Brunei	BSB
Brussels	BRS
Brussels	BRC
Brussels (USNATO)	BRU
Bucharest	BCH
Budapest	BDP
Buenos Aires	BNS
Bujumbura	BUJ
Bukavu	BUK
C	
Cairo	CRO
Calcutta	CLC
Calgary	CLG
Cali	CLI
Canberra	CNB
Cape Town	CPT
Caracas	CRS
Casablanca	CSB
Cebu	CBU

Chiang Mai	CHN
Chihuahua	CHA
Ciudad Juarez	CDJ
Cochabamba	CCH
Colombo	CLM
Conakry	CRY
Constantine	CON
Copenhagen	CPN
Cotonou	COT
Curacao	CRC
D	
Dakar	DKR
Damascus	DMS
Dar es Salaam	DRS
David	DAV
Dhahran	DHR
Dhaka	DHK
Djibouti	DJI
Doha	DOH
Douala	DOU
Dublin	DBL
Durban	DRB
Dusseldorf	DSS
E	

Edinburgh	END
F	
Florence	FLR
Frankfurt am Main	FRN
Freetown	FTN
Fukuoka	FKK
G	
Gaborone	GAB
Geneva	GVA
Genoa	GEN
Georgetown	GEO
Goteborg	GTB
Guadalajara	GDL
Guatemala	GTM
Guayaquil	GYQ
H	
Hague, The	HAG
Halifax	HLF
Hamburg	HMB
Hamilton	HML
Harare	HRE
Havana	HAV
Helsinki	HLS
Hermosillo	HER

Hong Kong	HNK
I	
Ibadan	IBA
Isfahan	ISF
Islamabad	ISL
Istanbul	ISL
Izmir	IXM
J	
Jakarta	JAK
Jerusalem	JRS
Jidda	JDD
Johannesburg	JHN
K	
Kabul	KBL
Kaduna	KAD
Kampala	KMP
Karachi	KRC
Kathmandu	KDU
Khartoum	KHT
Khorramsharr	KHR
Kigali	KGL
Kingston	KNG
Kinshasa	KIN
Kobe-Osaka (see Osaka-Kobe)	

Krakow	KRK
Kuala Lumpur	KLL
Kuwait	KWT
L	
Lagos	LGS
Lahore	LHR
La Paz	LPZ
Leningrad	LEN
Libreville	LIB
Lilongwe	LIL
Lima	LMA
Lisbon	LSB
Liverpool	LVP
Lome	LOM
London	LND
Luanda	LUA
Lubumbashi	LBM
Lusaka	LUS
Luxembourg	LXM
Lyon	LYN
M	
Madras	MDR
Madrid	MDD
Malabo	MBO

Managua	MNG
Manama	MNA
Manila	MNL
Maputo	MAP
Maracaibo	MRC
Marseille	MRL
Martinique	MRT
Maseru	MAS
Matamoros	MTM
Mazatlan	MAZ
Mbabane	MBA
Medan	MDN
Medellin	MDL
Melbourne	MLB
Merida	MER
Mexicali	MCL
Mexico City	MEX
Milan	MLN
Mogadiscio	MGD
Mombasa	MSA
Monrovia	MRV
Monterrey	MTR
Montevideo	MTV
Montreal	MTL

Morelia	MLA
Moscow	MOS
Munich	MUN
Muscat	MST
N	
Nagoya	NGY
Naha	NHA
Nairobi	NRB
Naples	NPL
Nassau	NSS
N’djamena	NDJ
New Delhi	NWD
Niamey	NMY
Nice	NCE
Nicosia	NCS
Nogales	NGL
Nouakchott	NUK
Nuevo Laredo	NVL
O	
Oporto	OPT
Oran	ORN
Osaka-Kobe	KBO
Oslo	OSL
Ottawa	OTT

Ouagadougou	OUG
P	
Pago Pago	PGO
Palermo	PLR
Panama City	PNM
Paramaribo	PRM
Paris	PRS
Peking (see Beijing)	
Perth	PRT
Peshawar	PSH
Piedras Negras	PDN
Ponta Delgada	PTD
Port-au-Prince	PTP
Port Louis	PTL
Porto Alegre	PTA
Port Moresby	PTM
Port-of-Spain	PTS
Port Said	PSO
Poznan	POZ
Prague	PRG
Praia	PIA
Pretoria	PRA
Puerto la Cruz	PLC
Q	

Quebec	QBC
Quito	QTO
R	
Rabat	RBT
Rangoon	RNG
Recife	RCF
Reykjavik	RKJ
Rio de Janeiro	RDJ
Riyadh	RID
Rome	RME
Rotterdam	RTT
S	
St. George	SGE
Saint John (New Brunswick)	STJ
St. John’s (Antigua)	SJS
St. John’s (Newfoundland)	SJN
Salsburg	SLZ
Salvador	SLV
Sana	S [sic]
San Jose	SNJ
San Louis Potosi	SNP
San Pedro Sula	SND
San Salvador	SNS
Santiago	SNT

Santiago de los Caballeros	SGO
Santo Domingo	SDO
Sao Paulo	SPL
Sapporo	SPP
Seoul	SEO
Seville	SVL
Shenyang	SNY
Shiraz, Iran	SHZ
Singapore	SGP
Sofia	SOF
Songkhla	SOK
Stockholm	STK
Strasbourg	STR
Stuttgart	STT
Surabaya	SRB
Suva	SUV
Sydney	SYD
T	
Tabriz	TBZ
TAI	TAI
Tampico	TMP
Tangier	TNG
Tegucigalpa	TGG
Tehran	THR

Tel Aviv	TLV
Thessaloniki	TES
Tijuana	TJN
Tokyo	TKY
Toronto	TRT
Trieste	TRS
Tripoli	TRP
Tunis	TNS
Turin	TRN
U	
Udorn	UDN
Valencia	VLC
Valletta	VLL
Vancouver	VAC
Veracruz	VRC
Victoria\	VTR
Vienna	VNT
W	
Warsaw	WRW
Wellington	WLL
Windsor	WND
Winnipeg	WNN
Y	
Yaounde	YDE

Z	
Zagreb	ZGB
Zanzibar	ZAN
Zurich	ZRH

12 FAM 539 EXHIBIT 539.2-3 STANDARD OPERATING PROCEDURES FOR TOP SECRET CONTROL OFFICERS

(TL:DS-61; 10-01-1999)

a. Top Secret Control Number composition:

Consecutive Number for Document TS Control Received			
Bureau/Office Number	Control Symbol	Year	Originated That Year
ARA-90/14	ARA	90	14

b. When more than one copy of a document is controlled, add a number suffix:

ARA-90/14-1
ARA-90/14-2
etc.

c. S/S uses a unique number system for all documents which pass through that office; it consists of the first two digits for the year and the remainder are for the next document processed: 9040560. The number is usually stamped, typed, or written on the document. When there is an S/S number, use it as your TS control number by placing your control symbol in front of it:

ARA-9040560

If you have more than one copy of the document, place the suffix after the number:

ARA-9040560-1
ARA-9040560-2

d. The TSCO must do any reproduction of Top Secret material. Prior to reproduction, verify that the document states that copies may be made or obtain authorization from the originator. Reproduction control is indicated

by adding an alpha/numeric suffix based on when reproduction is made and how many copies are made of a controlled document:

First reproduction = ARA-90/14-A/3
ARA-90/14-2-A/3
ARA-9040560-A/3

Second or more = ARA-90/14-B/3, Etc.

e. Upon receipt of a TS document: determine if it has a State office's control number on it. If it does, use it. If it does not, use your next consecutive number.

f. Type or write the control number on the document at the top right corner and used on the cover sheet and inventory record.

g. Control any TS documents attached as enclosures, attachments, tabs, etc., by using the same control number which will be placed at the top right corner as:

Atch/Encl/Tab To ARA-90/14

h. For TS documents originated by your office, ensure that a TS classifying authority (DAS or above) signs or clears on it. If it is only cleared, the first page must have the "classified by" line on it. All pages must be marked TS top and bottom. Declassification statement must be included. If possible, use an unclassified subject and mark it (U). Paragraph markings must be included. The document must come through you to check and control copy(s) which will be retained.

i. Do not control Sensitive Compartmented Information (SCI) or Special Access Program (SAP) material. These documents will have a suffix codeword or program indicator after the classification marking. SCI codeword HVCCO must be maintained in INR under different control procedures. SAP documents are controlled by a separate system, but may be stored locally if authorized by the SAP manager. Only SAP-indoctrinated personnel may have access to the container.

12 FAM 539 EXHIBIT 539.2-5 FORM DS-794, RECEIPT MANIFEST

(TL:DS-61; 10-01-1999)

U. S. DEPARTMENT OF STATE

RECEIPT MANIFEST

DATE

SENT TO

MANIFEST NUMBER

D

MESSAGE CONTROL NUMBERS

INCOMING	COPY NO.	OUTGOING	COPY NO.

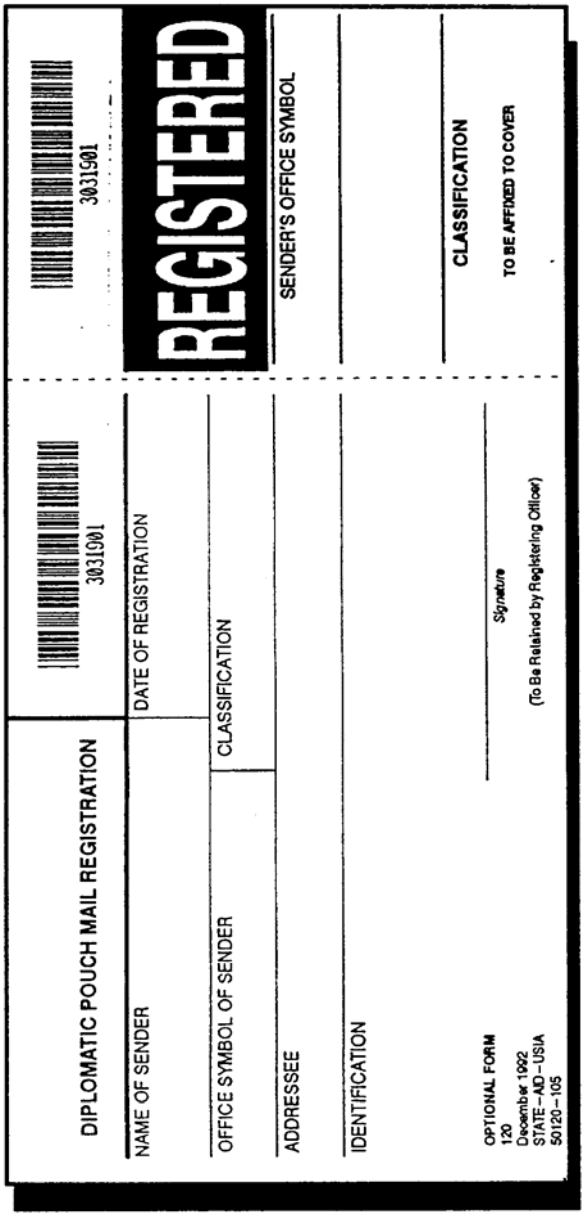
Sign receipt and return to SO/DO/CC/TOP, Room 5243, New State Building (or Tube Station D-1) within 24 hours.

(Signature)

FORM 11-89 DS-794

12 FAM 539 EXHIBIT 539.4-2 FORM OF-120, DIPLOMATIC POUCH MAIL REGISTRATION

(TL:DS-61; 10-01-1999)



DIPLOMATIC POUCH MAIL REGISTRATION

3031901

NAME OF SENDER

DATE OF REGISTRATION

OFFICE SYMBOL OF SENDER

CLASSIFICATION

ADDRESSEE

IDENTIFICATION

Signature

(To Be Retained by Registering Officer)

OPTIONAL FORM 120
December 1992
STATE–AID–USIA
50120–105

3031901

REGISTERED

SENDER'S OFFICE SYMBOL

CLASSIFICATION

TO BE AFFIXED TO COVER

12 FAM 539 EXHIBIT 539.5-2 JF-58, REGISTER-DESTRUCTION OF CLASSIFIED MAIL

(TL:DS-61; 10-01-1999)

REGISTER – DESTRUCTION OF CLASSIFIED MATERIAL
(NON-RECORD COPIES)

ORGANIZATION

DESTRUCTION DATE	CLASSIFICATION	COPY NUMBER (S)	DATE AND DESCRIPTION OF MATERIAL	SIGNATURE AND TITLE OF POSITION OF PERSON DESTROYING OR PREPARING FOR DESTRUCTION	SIGNATURE AND TITLE OF WITNESS

FORM JF-58
4-84