tion may be initiated. At this time, it will be determined which of the three Top Secret control officers will assume accountability for use and storage, and what Top Secret control number will be assigned if the document has been received without such number being assigned by the originator.

961.2-4 Top Secret Cover Sheets

The original and each copy of Top Secret documents must be covered by Top Secret Cover Sheet, OF-115. The cover sheet must be completed by the Top Secret control officer and shall 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 must sign and date the cover sheet before accepting responsibility for its custody. The Top Secret Cover Sheet must remain with the document until the document is:

a. Transferred to another agency;
b. Destroyed;
c. Retired;
d. Downgraded; or
e. Declassified.

When one of the above listed actions is taken, the Top Secret control officer must record the action on the Top Secret Cover Sheet, retain it in the files for 5 years, and then destroy it.

961.2-5 Distribution

a. Top Secret documents distributed outside the area of the Top Secret control officer must be covered by either a Classified Material Receipt, OF-112, or Receipt Manifest, DS-794, 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.

Top Secret control officers or designated alternates are responsible for the accountability, proper handling, and storage of Top Secret material. Distribution of Top Secret documents will be made only by the Top Secret control officer or alternate. All persons who read or who have access to a Top Secret document must sign their names 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 Top Secret control officer.

Direct receipt of Top Secret documents from outside the area by an employee other than the Top Secret control officer is not permissible under these regulations, and if a Top Secret document is received, it must be immediately turned over to the Top Secret control officer for appropriate accountability. No employee other than the Top Secret control officer will transfer Top Secret documents out of the area of jurisdiction.

b. In USIA and ACDA, Top Secret documents may be transmitted between Top Secret control officers or between a Top Secret control officer and an office head or higher authority of another element. In every case, the document's distribution and handling must be controlled and accounted for by a Top Secret control officer. The Top Secret control officer or the office head or higher authority will insure that distribution is limited to properly cleared employees.

961.2-6 Administrative Action

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 originating office's permission, or allows another employee who does not have a "need-to-know" to have knowledge of Top Secret information will be subject to administrative action which could consist of a letter of reprimand by the Director General or a suspension without pay. Gross disregard of these regulations could lead to dismissal or legal action.

962 METHODS OF TRANSMISSION OR TRANSPORTATION

962.1 Authorized Channels

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.

b. If classified material must be transmitted through U.S. mail or other postal services, it must pass through the central mail or pouch unit serving the post or area in the agency of the sender.

c. The "mail stop" interagency mail service is not an authorized messenger for delivery of classified material.

d. See Exhibit 962 on guide for transmission of classified mail.

962.2 Top Secret

Top Secret information must be transmitted by either:

a. Top Secret messenger;
b. Authorized courier; or
c. Electrical means in encrypted form.

962.3 Secret and Confidential

Secret and Confidential information should be transmitted, dependent upon the urgency of the information, the maximum security obtainable, and the medium available, by one of the means approved for Top Secret. Whenever one of the methods of transmitting Top Secret material (which are under the positive control of the Department or agency) are not readily available, the registered mail facilities of the United States and U.S. military postal channels can be used as follows:

a. 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.

b. 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.

962.4 Unclassified Material

At posts, 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 be transmitted through the official communications center serving the agency of the sender.

962.5 Preparation for Transmission

962.5-1 Envelopes, Containers, Covers

a. Classified documents must be covered by a cover sheet or folded inwards and be enclosed in opaque envelope. Material transmitted via pouch (i.e., by diplomatic courier), by authorized messenger, or by pneumatic tube 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.

b. An inner envelope should be addressed to the appropriate official by title if known. It must be marked on both sides with the appropriate classification. An outer envelope is required for U.S. mail and should be addressed in the same manner, but shall not bear a security classification or any other indication that the contents are classified. Envelopes must be completely and properly addressed and include the sender's return address.

962.5-2 Receipts and Registration

Top Secret and Secret material transmitted outside the organizational control of the sender must be receipted for by means of Classified Material Receipt, OF-112, Receipt Manifest, DS-794, or other receipt approved by the Office of Security or regional security officer. These receipts may be used for the transmission control of any other material at the discretion of the sender.

a. Use of Form OF-112

OF-112, *Classified Material Receipt, is prepared so that* all items are completed and signatures are recorded on parts I, III, and IV. These parts, together with part V, shall be retained for 2 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 addressee will be notified. In either case should the error not be resolved, *security personnel shall be notified.* 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.

b. Use of Form DS-794

Form DS-794, Receipt Manifest, or other approved receipt, is used 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. Such receipts are retained for 2 years.

962.5-3 Disposition of Receipts

Originating and receiving elements or employees are not required to maintain additional logs of transmission and receipt of Secret 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 Secret material, receipts covering the transaction may be destroyed.

962.5-4 Registering Diplomatic Pouch Mail

Each piece (envelope, package, or other outer cover) of classified material must be registered by the use of a OF-120, Diplomatic Pouch Mail Registration.

962.5-5 Transmission of Classified Demountable Magnetic Storage Media

Should it be determined that classified information resident on a magnetic storage media must be transmitted outside *of the Department or to another Departmental component* located in another geographical location, the data or word processing document must be copied to a new piece of magnetic storage media.

963 REPRODUCTION OF CLASSIFIED MATERIAL

963.1 *Policy*

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.

963.2 Reproduction of Top Secret Documents

Unless otherwise marked, permission for reproduction of a Top Secret document must be obtained by the Top Secret control officer of the reproducing office, from the Top Secret control officer of the originating office, or the Top Secret control officer 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, unless otherwise marked, the reproduction of Top Secret

material requires the approval of the Executive Secretary and such reproduction can be accomplished by the ES Staff only.

963.3 Reproduction of Secret and Confidential Documents

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

b. Unless otherwise marked, in AID/W, Secret telegrams and airgrams can only be reproduced by the Telecommunications Branch, SER/MO/CM. Requests for reproduction require the express approval on form AID 630-1 (Request to Reproduce Classified Documents) by an officer of the Office Director level or equivalent. Unless otherwise marked, reproduction of other Secret material and reproduction of all Confidential material require the express approval on form AID 630-1 by an officer of the Office Director level or equivalent.

963.4 Records of Reproduction

Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations. 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. For AID, this information will be marked on form AID 630-1.

963.5 Protection of Classified Reproduction Facilities

a. Classified reproduction facilities should be controlled and kept separate from unclassified operations and must be monitored periodically during normal working hours and secured within a locked room during nonworking hours. Where this is not possible, the Office of Security or regional security officer must be consulted in determining the procedures necessary to protect facilities used for classified reproduction.

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

964 DESTRUCTION OF CLASSIFIED MATERIAL

Disposable classified material must be carefully and completely destroyed only through authorized means by cleared U.S. citizen employees.

964.1 Destruction of Top Secret Material

964.1-1 Requirements

Top Secret control officers are required to record destruction of Top Secret material on corresponding Top Secret cover sheet and retain the cover sheet for 5 years.

964.1-2 Witness to Destruction

The Top Secret control officer in recording the destruction of a Top Secret document must sign form OF-115 as the officer destroying the document and one other 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 burnbags and securing the burnbags for destruction.

964.2 Destruction of Secret and Confidential Material

Records of destruction need not be made for Secret or Confidential material unless recording is required by special regulation. Destruction will be recorded on Register-Destruction of Classified Material, OF-114, or other form or log approved by the Office of Security or the regional security officer. 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.

964.3 Use of Burnbags

All classified material to include word processing multistrike ribbon containers and routine typewriter ribbon cartridges, to be destroyed must be placed in containers designated as burnbags, which are clearly and distinctly recognizable as burnbags. Burnbags awaiting destruction must be protected by safeguards commensurate with the classification designation of the material involved.

964.4 Methods of Destruction

Classified material is normally destroyed by burning or, with the exception of microforms, by disintegration. Any other method must have the approval of the Office of Security. 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 Departmental instructions.

964.5 Destruction of Classified Demountable Magnetic Storage Media

All demountable magnetic data and program storage media which have been used for processing classified data must be destroyed in accordance with established Departmental guidelines for the destruction of this media.

965 REPORT OF MISSION OR COMPROMISED CLASSIFIED DOCUMENTS

Any employee who discovers that classified material is missing or possibly compromised must make a prompt report to the Office of Security or regional security officer via the principal unit security officer or post security officer. In the case of Top Secret or cryptographic information or material, the report must be made immediately. Telegraphic or oral reports must be followed by a prompt submission of a memorandum addressed to the Office of Security or regional security officer, including the following information:

a. Complete identification of the information, including when possible, the date, subject, originator, address, serial or legend markings, classification, type of material (i.e., telegram, memorandum, airgram, etc.), and a damage assessment of the impact of the disclosure.

b. Where material is lost or missing, the narrative statement should detail the time, date, and circumstances under which the loss was realized; the recent handling of the material and the persons having access to it; and the steps taken to locate the material.

c. Where compromise is believed to have occurred, the narrative statement should detail the circumstances which gave rise to the compromise, the unauthorized person who had or may have had access to the information, the steps taken to determine whether compromise in fact occurred, and the office or post evaluation of the importance of the information compromised.

d. Where cryptographic information is lost or compromised, a telegraphic report is also to be made to the Office of Communications (OC/S) followed by a Report of Violation of Communications Security, FS-507.

e. If the potential compromise involves an automated information system, a telegraph report is also to be made to the Information System Security Staff (A/ISS).

966 REPORTING OF UNAUTHORIZED DISCLOSURES

966.1 General Procedure

All bureaus and posts must report actual or suspected disclosures of classified information to any unauthorized recipient.

Detailed reports of the circumstances surrounding each unauthorized disclosure must be promptly reported to the Deputy Assistant Secretary for Security and to the Director, Office of Security in USIA and AID, as appropriate, and in OPIC, the Vice President for Personnel and Administration.

966.2 Report of Unauthorized Disclosure

A report of unauthorized disclosure must provide the following:

a. Date the incident occurred, if known;

b. Identity of the document and the person or persons who furnished or disclosed the information (defined as any record information in any medium), if known;

c. Subject and security classification of the compromised information;

d. Identity of the publication (public press, technical journals, report, etc.), speech, or briefing containing the unauthorized disclosure or the unauthorized recipient of the classified information;

e. Include a damage assessment of the impact of the unauthorized disclosure both on the Government and upon the public;

f. Where appropriate, state action planned or taken to prevent similar disclosures or recurrences; and

g. Attach additional sheets or exhibits, as necessary.

967 through 969 (Unassigned)

A Guide for Transmission of Classified Mail[1]

CLASSIFICATION	With an Office Serviced by a Single Message Center	Between Offices, Areas, and Bureaus and Between State, AID, USIA	To Other Government Agencies and Within U.S. and its Possessions	Between Washington Offices and Posts, and Between Posts
LIMITED OFFICIAL USE	Envelope and receipt optional. If envelope used, mark classification front and back. Delivery by authorized employee[2] or messenger service.	Single addressed envelope with classification marked front and back. Outer cover as required by section 962.5-1 (pouch, messenger's portfolio, etc.). Transmission by authorized messenger.[2] "Mail Stop" system not authorized. Receipt optional.	Double addressed envelopes. Mark inner envelope with classification front and back. Register in central mail room. Transmission by U.S. registered mail or by authorized messenger.[2] "Mail Stop" system not authorized. Receipt optional.	Single addressed envelope marked with classification front and back. Outer cover as required by section 962.5-1 (courier pouch, etc.). To Pouch Room by authorized employee.[2] Transmit by diplomatic courier pouch. Receipt optional. Register using OF-120 (section 962.5-4).
CONFIDENTIAL	Same as above.	Same as above.	Same as above.	Same as above.
SECRET	Same as above. Distribution recorded. JF-60 or equivalent.	Same as above. OF-112 required.	Same as above except: Transmit by U.S. registered mail. OF-112 required. Parts I - III of OF-112 may be used with third envelope for control to mail room; Parts IV and V enclosed with document in inner envelope.	Same as above except: OF-112 required (section 962.5-2).
TOP SECRET (Sections 961 and 962)	Movement controlled by area Top Secret control officer. OF-115 cover sheet and Top Secret control number required. Distribution recorded. Use OF-112 or OF-116 as required by area Top Secret control officer. Delivery by authorized employee.[2]	Controlled by Top Secret control officers of sending and receiving organizations. Single addressed envelop with classification marked front and back. Outer cover as required by section 962.5-1 (pouch, messenger's portfolio, etc.) Of-115 required. OF-112 required. Delivery by Top Secret Messenger or authorized employee.[2]	Controlled by Top Secret control officers of sending and receiving organizations. Single addressed envelope with classification marked front and back. Outer cover as required by section 962.5-1 (courier pouch, etc.). OF-115 removed when sent to another agency outside State, AID, USIA. OF-112 required. Transmit only by official courier or authorized employee.[2]	Controlled by Top Secret control officers of sending and receiving organizations. Single addressed envelope marked with classification front and back. Outer cover as required by section 962.5-1 (courier pouch, etc.). OF-115 required. OF-112 required. Transmit by diplomatic courier.

[1] Consult text of 5 FAM 900 and central mail or records unit for additional guidance. Follow other procedures only as approved by the office of Security or regional security officer.

[2] Only E.O. 10450 cleared personnel may carry classified or controlled material.

970
PHYSICAL PROTECTION OF CLASSIFIED MATERIAL

971 STORAGE OF CLASSIFIED MATERIAL

(TL:CR-129 & SY-9 9-26-9)
(Uniform State/AID/USIA/ACDA/OPIC)

971.1 General Requirements

a. 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 exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. The requirements specified in this regulation represent the minimal acceptable standards and may be supplemented by additional safeguards which, at the discretion of the Office of Security or regional security officer, may be necessitated by unusual or changing conditions.

b. Classified material must not be routinely stored overnight at overseas facilities, unless there is present a satisfactory emergency destruction capability.

c. Whenever classified material is not under the personal control and observation of an authorized person, it will be stored in an approved locked container. Open storage of classified material in a vault, except shredded waste about to be destroyed and sealed diplomatic pouches, is not allowed unless specifically authorized in writing by the Office of Security and the Office of Communications.

d. All personnel handling classified and administratively controlled material are responsible for placing a cover sheet (JF-18) on the material to prevent unauthorized access and to alert personnel of the requirement for proper storage.

e. Responsibility for the secure storage of classified material in message distribution lockers (MDLs), which are located within post communications centers, rests with appropriate personnel from the office to which the locker is assigned.

971.2 Top Secret

a. Domestic

Top Secret documents must be stored in a General Services Administration (GSA)-approved, safe-type, steel file cabinet having a built-in three-way dial type combination lock and, where possible, located in an alarmed restricted area.

b. Overseas

Top Secret documents must be stored in a GSA-approved container with a three-way dial combination lock located in a security-approved vault in a building which has been accorded diplomatic status. PCC vault and privacy door combinations sealed in approved tamper-resistant packets issued by the Department, which are to be stored at MSG Post No. 1 in a GSA-approved safe container, are excepted from the vault storage requirement. Exceptions to the vault location requirement must be approved in writing by the Regional Security Officer. For AID and USIA overseas, no Top Secret documents are to be moved from Chancery to an AID or USIA facility.

971.3 Secret and Confidential

a. Domestic

Secret and Confidential documents may be stored in the manner authorized for Top Secret, or in a GSA-approved safe file, or in a barlock cabinet equipped with a security-approved combination padlock if the building is controlled by security cleared U.S. citizen personnel on a 24-hour basis.

b. Overseas

Secret and Confidential documents may be stored in the manner authorized for Top Secret, in a GSA-approved safe file, or in a barlock cabinet equipped with a security-approved combination padlock if the cabinet is located in a security-approved vault and/or in a restricted area to which access is controlled by U.S. citizen personnel on a 24-hour basis.

971.4 Storage of Classified Material by Persons Not Regularly Employed

Authorized consultants and contractors engaged in work involving classified information may not store such material overnight on their premises unless the Office of Security has granted approval for such storage. No classified information may be made available to consultants or contractors off the official premises or transmitted to such persons off the premises except with the approval of the Office of Security and in conformity with The Order, its implementing directives, and these regulations.

972 CHANGING COMBINATIONS

a. Combinations to security containers and doors will be changed only by individuals having an appropriate security clearance and the authority to have access to the combination. Post or Unit Security Officers and Communications Programs Officers will insure combinations are changed as Combinations will be changed under any of 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) At least once every 12 months, except for communication area vault doors which must be changed every 6 months; or

(5) When equipment is taken out of service.

b. Combinations must be recorded on a Combination Safe Card, OF-111. Records of combinations must be classified no lower than the highest category of classified material authorized for storage in the security equipment concerned. 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 Officer according to distribution instructions printed on the card. At a minimum, they must be stored in repositories authorized for the storage of material at the highest combined classification level to which combinations permit access. Except for the Combination Safe Card and cards posted inside repositories listing combinations in the immediate area, the recording of combinations is prohibited. Combinations must be committed to memory.

c. Combinations to repositories containing official funds are subject to the requirements of 4 FAM 317.3 and the instructions of the responsible regional security officer.

d. 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. Part 3 of OF-111 is designated for this purpose.

973 REMOVAL OF CLASSIFIED MATERIAL FROM OFFICIAL PREMISES

973.1 Overnight Custody

a. 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.

b. In unusual circumstances, requiring the overnight removal of classified material from official premises, prior approval from the Office of Security or the regional security officer is mandatory. This is to insure adequate storage measures and compliance with the Executive Order 12356, implementing directives, and other applicable regulations.

973.2 Certification Upon Permanent Departure From Post

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

a. Classified material is not being taken from the post through other than authorized means;

b. Such material is not in their household or personal effects; and

c. Such material will not be mailed or otherwise transmitted in violation of section 962.1.

This requirement is in addition to the Form OF-109, Separation Statement, required by 3 FAM 984.2-3.

974 SAFEGUARDING CLASSIFIED INFORMATION

974.1 General Procedures

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

b. Classified material must not be left in unoccupied rooms or be left inadequately protected in an occupied office, or one occupied by other than security cleared employees.

974.2 Precautions

a. "Open/Locked" signs should be used on every repository containing classified material to indicate that the repository is either open or locked.

b. A Security Check Sheet, OF-121, should be affixed to every repository containing classified material and employees opening or closing the container should complete the appropriate column. The security check sheet should also be used for classified word processing systems to insure that the classified information processed on such systems is properly secured and protected at the end of the business day.

c. Personnel must insure that classified repositories are locked prior to leaving the room unattended. When securing a combination lock, the dial must be turned at least four complete turns in the same direction after closing. The employee should double check the repository to insure that it has been properly secured.

d. Defects in or malfunctioning of storage equipment or locking devices must be reported immediately to the Office of Security or the post security officer. Uncleared personnel will not be permitted to service any equipment to be used for the storage of classified material.

e. Before taking security containers out of use, custodians must thoroughly inspect them to insure all classified material has been removed and a standard combination set.

974.3 After Working Hours and During Lunch Periods

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

b. Classified material, including disposable material such as rough drafts, shorthand notes, extra carbon or tissue copies, used carbon paper, hectograph masters, and mimeograph stencils, must be safeguarded and locked in appropriate security repositories whenever unattended. All typewriter ribbons and voice recording materials must be safeguarded and locked in appropriate security repositories at the close of business. Compliance with this requirement is a sound security practice and and is advantageous to efficient administrative operations regardless of whether the media contain classified information. For these same reasons, a "Clean Desk" policy of securing all classified and unclassified documents is strongly encouraged.

c. All keys to doors kept locked after working hours must be turned in to U.S. citizen guard force and released only to

authorized personnel. Where no U.S. citizen guard force is assigned, personal custody of keys may be authorized by Office of Security or regional security officer. Such instances should be held to an absolute minimum.

974.4 Closing Hours Security Check

974.4-1 OF-122, Report of Closing Hours Security Checks

a. A system of security checks prior to those conducted by security guards should be instituted at the close of each working day, or as soon thereafter as administrative operations permit. Such a system ascertains that all classified material, to include that processed on any automated information system, has been properly stored and that containers are locked; that windows and doors, where appropriate, are locked; and that the area is otherwise secure and not susceptible to overt penetration.

b. In order to fulfill this fundamental, mandatory requirement in all areas, at all echelons, supervisory officers in the United States and at posts 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 OF-122, Report of Closing Hours Security Check, to record the results of the closing hours security check and forward it to the unit or post security officer upon completion of the final check.

974.4-2 Reporting Infractions

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 Security Violation, unless higher administrative authority determines otherwise or the closing hours security check is, in fact, the final inspection where U.S. citizen guards or U.S. Marines are not on duty.

974.4-3 Employee Responsibility

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

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

(2) Check the tops of all desks, including "in" and "out" boxes, and repositories to insure that all classified and controlled material has been put away; and

(3) 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 AID, the checker may be jointly charged with the violation.

974.4-4 Exceptions to Requirements

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 the Office of Security or regional security officer.

974.5 Conferences

a. In conducting conferences where classified information or material may be involved, every precaution should be observed to insure that:

(1) In the interests of technical security, classified conferences are held 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. Advance notice to (and coordination with) the appropriate post or regional security officer or Office of Security should be given by the operations element calling or conducting the conference 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 appropriate security clearance by the officer calling or conducting the classified meetings except when the participants are U.S. citizen employees of the Department, AID, OPIC, and USIA, or regularly assigned U.S. personnel at diplomatic and consular posts.

975 PHYSICAL SECURITY

975.1 Cameras

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

975.2 Package Control

In unusual or emergency circumstances, the Office of Security or regional security officer, with the approval of higher authority, may impose such restrictions as deemed appropriate to insure that foreign objects are not introduced into U.S. Government facilities or classified material is not removed.

975.3 Identification of Employees

Official employee identification cards are issued and controlled by the Office of Security or regional security officer.

975.3-1 Entry of Employees in Buildings

Employees must present authorized identification cards to guards, receptionists, and/or other employees on request when entering buildings or restricted areas at any time.

975.3-2 After Hours Access to Buildings

a. In addition to showing proper identification, all employees shall be required to sign a register when entering or leaving a building outside of regular working hours.

b. When foreign national employees are required to work after hours in post buildings and when nonregular employees, contractors, etc., are required to enter or remain in buildings after working hours, the U.S. officer authorizing the work must obtain the concurrence of the Office of Security or regional security officer or the post security officer. Such

persons must sign in and out on the appropriate register. Nonregular employees and contractors must be escorted.

975.3-3 Loss of Identification Cards

When an employee identification card is lost in Washington, a memorandum report must be submitted immediately to the Identification Unit, Office of Security. A card lost at a post must be reported immediately to the Identification Unit, Office of Security, through the post's administrative officer. In each case, the report should include a statement of the circumstances surrounding the loss and the details of any efforts to recover the card. (See 3 FAM 094.6 and 1566.)

975.4 Entry of Visitors

Visitors are not permitted in any building housing classified material or operations after working hours, unless they are escorted by a U.S. citizen employee. Normally, after working hours visitors are required to register at the guard desk.

976 SECURITY PLANS FOR OFFICE MOVES

A security plan must be devised by the unit or post security officer concerned to insure that proper security measures are observed during office moves. The security plan must then be forwarded to the Office of Security or regional security office well in advance of the intended move. It should include provisions for assuring that repositories of classified material are securely locked, and that a means is provided for accounting for their dispatch and receipt by a designated U.S. citizen employee. While in transit, repositories containing classified material must be accompanied by a U.S. citizen employee. Prior to the execution of any lease for functional space where there will be classified material and/or classified operations, security requirements should be coordinated with the Office of Security or the responsible regional security officer.

977 through 979 (Unassigned)

980
COMMUNICATIONS SECURITY (COMSEC)

981 AUTHORITY

(TL:CR-129 & SY-9 9-26-85)
(Uniform State/AID/USIA/ACDA/OPIC)

a. Heads of the independent departments and agencies have responsibilities for executing all measures required to ensure the security of Federal telecommunications.

b. Cryptographic information and all material used in the encryption or decryption of telegrams are protected by law. (See 18 U.S.C. 798 and 952, as quoted in 5 FAM 900, Appendix IV.)

982 RESPONSIBILITIES

982.1 Communications Security Division (OC/TS/S)

The Office of Communications, Communications Security Division, is responsible for the development of regulations and procedures for the control of communications security and is responsible for prescribing or approving all systems and techniques used in any manner to assure the security of telecommunications. Included are the application of protective measures to telecommunications systems and facilities and establishments of regulations and procedures governing the operations, use, modification, or removal from use of such systems and techniques.

982.2 Communications Security (COMSEC) Officer

982.2-1 Designation

The principal officer at each post and the officer in charge of a major functional area at Washington, D.C., holding cryptographic or other communications security material must appoint a COMSEC officer or personally act in that capacity. A current cryptographic clearance is a prerequisite to appointment.

982.2-2 Responsibilities

The COMSEC officer is responsible for insuring that the communications security regulations and procedures are observed at the post or unit, and for the prompt investigation and submission of reports regarding violations. The detailed responsibilities of the COMSEC officer are contained in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

982.2-3 Violations

Any violation of communications regulations or procedures which may affect the security of telecommunications is a communications security violation and must be reported by COMSEC officers to the Communications Security Division (OC/TS/S) on Form FS-507, Report of Violation of Communications Security. When such a violation may have resulted in the compromise of classified or administratively controlled information, the initial report must be by official telegram from posts, or by telephone from those units at Washington, D.C. Detailed instructions on the reporting of cryptographic and other communications security violations are contained in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian. (See also sections 965 and 994.)

982.3 Communications Security (COMSEC) Custodian

982.3-1 Designation

The principal officer at each post and the officer in charge of a major functional area at Washington, D.C., holding cryptographic or other communications security material must appoint an employee to serve as COMSEC custodian and one or more employees to serve as alternates, or must personally act as COMSEC custodian and appoint an alternate(s). A current cryptographic clearance is a prerequisite to appointment. The appointment is to be documented on Form JF-47, Appointment of COMSEC custodian; the original copy is to be forwarded to the Communications Security Division (OC/TS/S) and a copy retained with COMSEC account records. Personnel of other agencies are not to be appointed either COMSEC custodian or alternate. Submission of a new or revised JF-47 supersedes all others previously submitted; therefore, it is necessary to reaffirm all appointments when there is a change in any appointment.

982.3-2 Responsibilities

The COMSEC custodian is held personally responsible for all material issued to the COMSEC account. The detailed responsibilities of the COMSEC custodian are contained in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

982.3-3 Transfer of Custody

At least 30 days prior to a custodian's departure from the assignment, a new custodian is to be appointed. Both the incoming and outgoing custodian are to conduct an inventory by sight-checking all material and are to submit a report on SF-153, COMSEC Material Report, to document the transfer of accountability in accordance with section 986.6.

The COMSEC Central Office of Record (COR) is to verify the report with its records and is to relieve the custodian formally of accountability for the material when any discrepancies have been resolved. The new custodian assumes responsibility for all material present in the account as of the time the new custodian signs the report.

983 TRANSMISSION OF CLASSIFIED AND ADMINISTRATIVELY CONTROLLED TELEGRAMS

983.1 Electrical Transmission

Classified or administratively controlled telegrams must be encrypted before transmission by any exposed communications channel.

983.2 Transmission by Pouch or Mail

a. Plain text copies of classified or administratively controlled telegrams must be transmitted in accordance with the regulations for other documents of similar classification or control designation.

b. A cipher text may be transmitted by unaccompanied pouch or by any postal facility. Delivery can frequently be expedited by this means when courier-accompanied pouch service is not available. Inquiries regarding this type of transmission must be made to the agency or post communications center.

984 PROTECTING CLASSIFIED AND ADMINISTRATIVELY CONTROLLED TELEGRAMS

Sections 950, 960, and 970 contain the regulations regarding safeguarding and dissemination of classified and administratively controlled information in any form. No special regulations are applied to the handling, use, physical storage, downgrading and declassification, dissemination, or reproduction of telegrams.

985 CRYPTOGRAPHIC CLEARANCE

a. Cryptographic material holds the key to the information contained in classified or administratively controlled telegrams and requires a high degree of protection. Authorization for access to and/or use of cryptographic material, therefore, must be limited and controlled.

b. Cryptographic clearance is the necessary, specific formal authorization for access to cryptographic information.

c. Principal officers, by virtue of appointment and office, have cryptographic clearance and no formal grant of clearance is necessary.

d. Persons possessing cryptographic clearance have such access on a "need-to-know" basis only.

985.1 Responsibility for Clearance

The Office of Communications will grant the formal clearance and forward necessary notification for those employees requiring cryptographic clearance provided they meet the established criteria. Cryptographic clearances remain valid as indicated in section 985.4, except that they may be revoked for cause.

985.2 Criteria for Clearance

Each employee who is to use and/or have access to cryptographic systems and cryptographic information must be a U.S. citizen and must have a clearance for access to Top Secret information based on a full field background investigation.

985.3 Categories of Clearance

Cryptographic clearance falls into two categories:

985.3-1 Cryptographic Clearance for Use

"Cryptographic Clearance for Use" is the prerequisite to and authorization for operation, keying, and maintenance of cryptographic systems and equipment issued by the Department of State.

985.3-2 Cryptographic Clearance for Access

"Cryptographic Clearance for Access" is the prerequisite to and authorization for access to crypto information, but does not constitute authorization for use of crypto keying material issued by the Department of State.

985.4 Effective Period

985.4-1 "Access" Category Clearance

Cryptographic clearance for access is valid only for the duration of the assignment of the individual to a given post, except that it may be revoked earlier for cause. For this purpose, consecutive tours of duty at the same post will be considered one assignment.

985.4-2 "Use" Category Clearance

a. Professional Communicator: Cryptographic clearances for use granted to professional communicators are valid for as long as the individual remains a professional communicator, except that it may be revoked earlier for cause.

b. All Others: The "Use" category cryptographic clearance granted to all other personnel is valid only for the duration of their assignment to a given post, except that it may be revoked earlier for cause.

985.4-3 Temporary Clearance

A temporary cryptographic clearance of either the "Use" or "Access" category granted by a principal officer during an emergency is valid only for the duration of an emergency.

985.5 Cryptographic Clearance for Use

All Clearances in this category must be formally granted by the Department, except that in an emergency the principal officer may grant temporary "Cryptographic Clearance for Use" in accordance with section 985.5-3. Each employee cleared for use must be adequately trained in the cryptographic systems to be used and must maintain a working familiarity with communications duties as long as a "use" category clearance is held. Failure to do so constitutes just cause for revocation of clearance.

985.5-1 Employees Trained for Cryptographic Duties

a. The Department initiates action covering an employee trained in the Department for cryptographic duties and notifies the post or the appropriate operational unit in the United States that "Cryptographic Clearance for Use" has been granted.

b. The post should request Departmental training for personnel who are or will be designated by the principal officer to serve as part-time or relief communicators before arrival at post so as to avoid on-the-job training.

985.5-2 Directors of Communications and Communications Electronics Officers

The Department initiates action covering Directors of Communications and Communications Electronics Officers and notifies the post of assignment, and all posts to be visited in line of duty, that "Cryptographic Clearance for Use" has been granted.

985.5-3 Temporary Cryptographic Clearance for Use

The principal officer in an emergency may grant a temporary "Cryptographic Clearance for Use" in writing to any U.S. citizen employee of the executive branch of the U.S. Government who is cleared for access to Top Secret information. The principal officer must inform the Communications Security Division (OC/TS/S) by telegram designated "Limited Official Use" at the time clearance is granted. The notification must provide the name and date of birth and justification for such authorization and the anticipated duration.

985.5-4 Requests for Cryptographic Clearance for Use

a. Requests for "Cryptographic Clearance for Use" for those persons not specifically assigned to communications duties, but who may be required to key cryptographic equipment, are directed to the Communications Security Division (OC/TS/S). No person can be allowed to key such equipment before receipt of "Cryptographic Clearance for Use." When clearance is received, such employees must be trained in keying by qualified personnel.

b. The principal officer at a post having no more than two employees assigned to cryptographic duties may, within the limits of post resources, designate at least one other person for part-time or relief cryptographic work. The principal officer must request "Cryptographic Clearance for Use" for employees so designated. Part-time or relief cryptographic personnel may not assume these duties before receipt of "Cryptographic Clearance for Use" from the Communications and Security Division (OC/TS/S). When such clearance is received, these employees must be trained on the job by qualified cryptographic personnel and be required to maintain a working familiarity with their cryptographic duties. Continuation of clearance is contigent upon successful completion of on-the-job training. At the conclusion of the training, the post must certify to OC/TS/S whether or not a satisfactory level of proficiency in communications operations has been reached.

c. Requests for "Cryptographic Clearance for Use" are to be submitted to OC/TS/S, giving the full name, date of birth, grade, and function of the person for whom clearance is requested.

985.6 Cryptographic Clearance for Access

a. Clearances in this category must be formally granted by the Communications Security Division, except as specified in section 986.6-6.

b. All persons, with the exception of the Principal Officer, having a cryptographic clearance for access must be escorted while in the PCC. As a matter of courtesy, the CPO should attend while the Principal Officer is visiting the PCC.

985.6-1 Foreign Service Inspectors, Public Members of Inspection Teams, Professional Security Officers, and Auditors

The Department initiates action covering auditors, Foreign Service inspectors, public members of inspection teams, and representatives of the Office of Security, such as regional security officers, technical security officers, etc. The Department notifies the post of assignment (and/or posts to be visited in line of duty) that "Cryptographic Clearance for Access" has been granted.

985.6-2 Personnel of the Office of Communications and the Office of Security

The Department initiates action covering personnel of the Office of Security and the Office of Communications who do not have "Cryptograhic Clearance for Use." These persons may not have access to cryptographic material and/or information until formal "Cryptographic Clearance for Access" is forwarded to the office or division in which they are employed.

985.6-3 Post Security and COMSEC Officers

In order to perform their assigned functions, the designated post security and COMSEC officers require cryptographic clearance. If they do not already possess either of the two categories of cryptographic clearance, "Cryptographic Clearance for Access" must be requested for them in accordance with section 985.6-6.

985.6-4 Other Persons

Requests for "Cryptographic Clearance for Access" for any other persons whose duties require access to cryptographic material and/or information are to be directed to OC/TS/S.

985.6-5 Requests for Cryptographic Clearance for Access Only

Requests for "Cryptographic Clearance for Access" are to be submitted to OC/TS/S, giving the full name, date of birth, grade, and function of the person for whom clearance is requested and a justification for the request.

985.6-6 Temporary Cryptographic Clearance for Access

a. The principal officer in an emergency may grant a temporary "Cryptographic Clearance for Access" in writing to any U.S. citizen employee of the executive branch of the U.S. Government who is cleared for access to Top Secret information. The principal officer must inform OC/TS/S by telegram designated "Limited Official Use" at the time clearance is granted. The notification must provide the name and date of birth and justification for such authorization and the anticipated duration.

b. Concurrent with a request to OC/TS/S for formal clearance, the principal officer may grant temporary "Cryptographic Clearance for Access" to employees having management or supervisory responsibility for communications, provided such employees meet the criteria in section 985.2. When such a clearance has been granted, state so in the request to OC/TS/S for formal clearance.

986 COMSEC MATERIAL CONTROL

The COMSEC material control system is designed to afford maximum physical security consistent with maximum utilization of communications security material through positive and continuing control during its production, storage, handling, physical transmission, and disposition. The systems management function and the special measures prescribed governing access to and physical transmission of storage, destruction, and accountability of COMSEC material are the means by which the control is to be established and maintained. Material is placed in and controlled within the COMSEC material control system for one or both of the following reasons:

a. Security Control

Because of the sensitive nature of the material, increased protection is mandatory.

b. Operational Control

Material requires special safeguards to insure it is readily available in the event of need for utilization.

986.1 Management of COMSEC Systems

The Communications Security Division (OC/TS/S) is responsible for managing the COMSEC assets of the Department of State to insure the proper and most effective use of the equipment and materials involved. Requests must be submitted to and approved by OC/TS/S prior to a transfer or issue of new or existing equipment or material accounted for in the COMSEC material control system except in an emergency involving safety of human life or the COMSEC material. Requests for a change in types of COMSEC equipment or material or services to satisfy new or changing requirements are to be submitted to OC/TS/S for approval. Specific information can be found in the current edition of the publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.2 Access to COMSEC Material

Access to COMSEC material or information requires that the individual possess a security clearance equivalent to the level of classification of the material, and a need-to-know. In addition, access to cryptographic information requires formal authorization in the form of a cryptographic clearance granted in accordance with section 985.

986.3 Transmission of COMSEC Material

986.3-1 Authorization for Transfer

Except in an emergency, only the COMSEC custodian or alternate, with prior OC/TS/S approval, is to transfer COMSEC material either within or outside the post or unit of assignment or responsibility. In an emergency, preferably the COMSEC custodian or alternate should transfer COMSEC material.

986.3-2 Package Preparation

All packages or envelopes containing accountable COMSEC material are to be marked or stamped "TO BE OPENED ONLY BY THE COMSEC CUSTODIAN" and are to be registered (using OF-120). Packages or envelopes containing cryptographic material (that is, COMSEC material bearing the marking "CRYPTO") or other classified COMSEC material bearing an accounting or register number are to be stamped or marked "TOP SECRET" if the material is Top Secret, or stamped or marked "Requires Handling as TOP SECRET" if the material is classified lower than Top Secret. Packages or envelopes containing accountable COMSEC material that does not bear an accounting or register number are to be marked or stamped with a classification reflecting the classification of the contents. Additional information is found in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.3-3 Method of Transmission (Shipment)

Cryptographic material (that is, COMSEC material bearing the marking "CRYPTO") and other classified COMSEC material bearing an accounting or register number are to be transmitted in the custody of and under constant surveillance of a courier designated or approved by the Department for the handling of Top Secret material, using handling procedures specified for Top secret material in section 962. Accountable COMSEC material that does not bear an accounting or register number is to be transmitted using the same method as for other information of equal classification, except that the package is to be registered (using OF-120, Diplomatic Pouch Mail Registration). Additional information is found in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.4 Storage of COMSEC Material

986.4-1 General

All cryptographic material (that is, COMSEC material bearing the marking "CRYPTO") and other COMSEC material bearing an accounting or register number must be stored as specified in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

All other COMSEC material is to be stored in the same manner as non-COMSEC material of equal classification.

986.4-2 Vault Area

"Open storage" of COMSEC or crypto keying material, when not in use or during closure hours, is not permitted even though the post communications center is or is not considered a "vault" area.

986.5 Destruction of COMSEC Material

986.5-1 Routine

When destruction is authorized, accountable COMSEC material is to be destroyed beyond any possibility of recovery by two persons possessing a current cryptographic clearance and the destruction is to be documented (see section 986.6). The destruction of certain types of COMSEC material requires that the COMSEC custodian be one of the persons. Additional information is found in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.5-2 Emergency

All employees whose activities include conducting cryptographic operations and/or holding classified COMSEC material must consider and plan for the possibility of an emergency which could expose COMSEC material to possible compromise. Plans must be made, and facilities provided, which will prevent entirely, or at least minimize, the extent and effects of such a compromise.

A destruction plan must be formulated by the COMSEC officer in conjunction with the security officer at each post. The necessary equipment must be readily available to effect the destruction of COMSEC material and equipment in an emergency. Specific guidelines pertinent to all aspects of emergency planning and execution, including types of emergencies, the emergency plan, precautionary destruction priorities, and necessary reports, are found in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.6 Accountability of COMSEC Material

986.6-1 COMSEC Central Office of Record (COR)

A COMSEC accounting system is to be maintained by the COR in the Communications Security Division (OC/TS/S) to provide rapid and accurate identification and location of all COMSEC material held by any organizational element within the Department.

986.6-2 COMSEC Accounts

A COMSEC account is to be established and maintained by the COMSEC custodian and one or more alternates at each post and major functional areas at Washington, D.C., holding communications security material. The COR is to establish regulations and procedures for operation of each COMSEC account to provide a uniform reporting and inventory system which will permit a complete "audit trail" of every item of COMSEC material. The detailed regulations and procedures are located in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.6-3 COMSEC Transaction Reports

In order that a complete record may be maintained of each COMSEC item, reports must be made on Form SF-153, COMSEC Material Report, or other form specified by the COR to record each transaction (e.g., shipment, inventory, destruction, transfer of custodian) involving the material. The reports are to be prepared and forwarded to the COR in OC/TS/S in accordance with instructions detailed in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

986.6-4 Periodic Physical Inventory

Inventories are required for physical security and COMSEC material management reasons. In accordance with the detailed instructions in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian, a complete physical inventory of each COMSEC account is to be conducted periodically, whenever there is a change in COMSEC custodians (see also section 982.3c), during regularly scheduled security surveys by the regional security officer, or as directed by the COR. The periodic inventory, on the specified date, is to be conducted by the COMSEC custodian of the account and another individual possessing a current cryptographic clearance. In an inventory, both individuals are to sight-check each item in the account as the basis for signing the certification required by the instructions in the current edition of the COMSEC publication titled "S/KAG-1" obtainable from the COMSEC custodian.

987 ACCESS TO PCC

a. Only individuals whose duties require it and who have been specifically authorized by the principal officer may enter the PCC. The names of personnel authorized to enter this room during normal operations must be posted inside the PCC entrance. The list must include all regular employees assigned to the PCC as well as those whose duties may require occasional admittance during normal operations. Individuals listed must have a Department of State cryptographic clearance or be a U.S. citizen employee of the executive branch of the U.S. Government with Top Secret clearance and be formally authorized access to cryptographic information by the employing department or agency. Verficiation of Top Secret clearance and verification of authorization for access to cryptographic information must be obtained, in writing, before allowing those individuals access to the PCC. Such employees of other agencies are not to have access to telegrams, particularly those bearing restrictive captions, or physical access to cryptographic keying material issued by the Department of State on the basis of being granted access to the PCC.

b. U.S. citizen employees of the executive branch of the U.S. Government not included on the authorized entrance list must meet access requirements prescribed in appropriate communications security publications, and must be specifically authorized by the principal officer to enter the PCC.

c. Non-U.S. citizen personnel access to PCC is covered in appropriate communications security documents obtainable from the COMSEC custodian.

988 UNAUTHORIZED MATERIAL

*Equipment, devices, materials, or codes and authentica*tion schemes intended to provide security, privacy, or authentication to information transmitted by electrical means (radio, telephone, wireline, etc.) not furnished or authorized for use by the Communications Security Division are not to be used.

989 (Unassigned)

990
ADMINISTRATION OF SECURITY REGULATIONS

991 OFFICE OF SECURITY

(TL:CR-129 & SY-9 9-26-85)
(Uniform State/AID/USIA/ACDA/OPIC)

The Office of Security is responsible for developing, defining, inspecting, and advising on facilities, procedures, and controls for safeguarding classified information, and for the enforcement of these regulations as they pertain to the domestic and overseas services. It establishes inspection programs and maintains active training and orientation programs for employees involved with classified information to impress upon each employee individual responsibility for exercising vigilance and care in complying with the provisions of these regulations. These programs include a continuing review of the implementation of these regulations to insure that national security information is properly safeguarded.

991.1 Office of Communications

The Office of Communications, within the Department is responsible for providing facilities to afford protection in transit of classified information transmitted electrically and via diplomatic courier pouches. It establishes and maintains communications security procedures and controls for the use of these facilities. It administers a training program for personnel assigned to communications duties.

991.2 Information System Security Staff

The Information Security Staff (A/ISS) is responsible for developing, coordinating, interpreting, and maintaining Department automation security policies, regulations, standards, and guidelines for the protection of classified and non-classified but sensitive information. It also performs security inspection studies, evaluations, and risk assessments of Departmental automated information systems and installations. A/ISS maintains current knowledge of automation security techniques applicable to the protection of classified data resident on automated information systems.

991.3 Regional Security Officers

Under the direction of the Deputy Assistant Secretary for Security, regional security officers assist and advise principal officers in discharging security responsibilities. They assist and advise post security officers and conduct security surveys of all overseas establishments, including facilities occupied by personnel of other Federal agencies under the jurisdiction of the principal officer.

992 POST SECURITY PROGRAM

992.1 Designation of Post Security Officers

a. A post security officer must be designated by the principal officer at each post to assist in carrying out the post's security responsibilities. At a post where a regional security officer is stationed, that officer assumes the functions of the post security officer.

b. At a post where a regional security officer is not stationed, the administrative officer should generally be designated as the post security officer. Written notification of post security officer designations and changes must be made to the appropriate regional security officer.

c. At larger posts, the post security officer determines the number of unit security officers required and their individual areas of jurisdiction. Designation of AID and USIA unit security officers overseas must be made with the concurrence of the principal AID and USIA officer at post.

992.2 Responsibilities of Post and Unit Security Officers

Employees designated as post or unit security officers perform the security duties prescribed for them in addition to the duties of their regular positions. Each post security officer maintains an active training and orientation program at the post to impress each employee with individual responsibility for exercising vigilance and care in complying with the provisions of the security regulations. The post security officer maintains liaison with the regional security officer and otherwise assists in the general administration of the security program within the assigned area of jurisdiction. In addition, the post security officer performs the specific duties prescribed in the various parts of the regulations and in the Post Security Officer Handbook, and such other security duties as may be required by the regional security officer.

993 DOMESTIC SECURITY PROGRAM

993.1 Designation of Principal Unit Security Officers

A principal unit security officer must be designated by the head of each major functional area to assist in carrying out the area's security responsibilities. Written notification of principal unit security officer designations and changes must be made to the Office of Security. Principal unit security officers of larger functional areas may designate and direct assistant unit security officers to carry out security responsibilities.

993.2 Duties and Responsibilities of Unit Security Officers

Employees designated as unit security officers perform the duties prescribed for them in addition to the duties of their regular positions. Each unit security officer maintains an active training and orientation program for employees of the unit area and impresses each such employee with individual responsibility for exercising vigilance and care in complying with the provisions of the security regulations. The unit security officer maintains liaison with the Office of Security and otherwise assists in the general administration of the security program within the assigned area of jurisdiction. In addition, to the general duties and responsibilities set forth above, such officer performs the specific security duties prescribed in the various parts of these regulations and such other security duties as may be prescribed.

994 SECURITY BRIEFING OF EMPLOYEES

994.1 New Employees

All employees must be afforded in-depth security briefings on these regulations which implement The Order and its implementing directives. Each new employee is required to read and sign a Security Acknowledgement (OF-110) at the time of entrance on duty.

In addition, it is the responsibility of post and principal unit security officers to insure that all newly assigned or newly employed personnel are briefed on security matters specific to a post or area.

994.2 Separating Employees

a. A security briefing will be conducted and a separation statement will be completed whenever an employee is terminating employment or is otherwise to be separated for a continuous period of 60 days or more. The briefing is mandatory to insure that separating personnel are aware of the requirement to return all classified material to official custody and of a continuing responsibility to safeguard their knowledge of any classified information. The separating employee must be advised of the applicable laws on the protection and disclosure of classified information (see Appendix IV) before signing the Separation Statement (OF-109).

b. A security debriefing will be conducted by the Office of Security, IG/SEC, upon the separation of AID employees.

995 SECURITY VIOLATION PROGRAM

995.1 General Policy

a. The Security Violation Program is designed to minimize the possibility of compromise of classified material.

b. A security violation occurs when classified material is not safeguarded in accordance with these regulations. *It is a security violation to process classified information on an unclassified system.*

995.2 Security Inspections

995.2-1 Domestic

Cleared U.S. citizen Federal protective officers, contract guards, and other persons specifically designated by the Office of Security are responsible for making after hour inspections to insure that these regulations for safeguarding classified material are being properly observed. Their official duties authorize their entry into any unoccupied or unprotected office at any time. Employees are prohibited from locking desk drawers.

995.2-2 Overseas

Marine Security Guards and persons specifically designated are responsible for making inspections during and after hours to insure that these regulations for safeguarding classified material are being properly observed. Their official duties authorize their entry into any unprotected office at any time. They are authorized to search desk drawers, unprotected boxes, attache cases, and review information resident on automated information system. Employees are prohibited from locking desk drawers.

995.3 Reports of Violations

995.3-1 Notice of Violation

Guards, employees specifically designated for security functions (excluding the closing hours security checker, when subsequent inspection will be conducted), and Regional Communications Programs Officers must submit a Notice of Security Violation (OF-117), identifying apparent violations, to the next higher level in the chain of security. The Notice of Violation report must be unclassified and must be prepared as comprehensively and accurately as possible, because it is the basis of any subsequent investigation. In addition, any employee must inform the appropriate security officer, orally or in writing, of any improper security practice which comes to the employee's attention in order that remedial action may be taken.

995.3-2 Record of Violation

a. When a Notice of Violation (OF-117), or other report from an employee, is received, the post or unit security officer must investigate the violation to determine the possibility of compromise and to identify the person(s) responsible for the violation. On conclusion of the investigation, the post or unit security officer will indicate the results in a brief summary on a Record of Violation (OF-118). The Record of Violation must be unclassified and include at a minimum, the information required to respond to the instructions printed on the reverse side. If necessary, classified or extensive additional information may be added on an attached memorandum.

b. On conclusion of the investigation and after Part 1 of the Record of Violation has been completed by the post or unit security officer, the Record of Violation will be forwarded to the person(s) alleged to be responsible, for completion of Part 2 of the report. The individual(s) alleged to be responsible may comment on the violation if desired, but is required to sign in Part 2, whether any comments are made or not. After the person(s) suspected of the violation signs in Part 2, the Record of Violation will be forwarded to the immediate supervisor for signature.

c. In domestic service, when the supervisor has signed in Part 2, the Record of Violation will be forward for adjudication in the Department to A/SY/OPS/DO, in AID to AG/SEC, in OPIC to the Office for Personnel and Administration, or in USIA to M/SP. Overseas, the Record of Violation will be forwarded to the regional security officer for completion of Part 3 of the form. On completion of Part 3 by the regional security officer, the original report will be forwarded to A/SY/OPS/DO and a copy to the employee.

d. Any substantive conflicting disclaimer or statement of mitigation in Part 2 of the OF-118 must be resolved or responded to by the regional security officer in Part 3 before forwarding the report to A/SY.

e. Record of Violation reports, in all cases, will be made a matter of record pending final adjudication and at posts a copy of the report will be placed in the post violation file. If, after adjudication, it is determined that a security violation should not be charged to the employee, the Office of Security will so notify the employee and instruct the unit, post, or regional security officer concerned to amend their records accordingly.

995.4 Violations by Employees of Other Agencies

Violations are reported and processed for employees of other Federal agencies in the same manner as above.

995.5 Evaluation of Security Violations

All reports of infractions of the security regulations will be evaluated initially by the post or unit security officer (except communications security violations) to determine whether or not a violation may have occurred. If a violation has occurred, the Record of Violation will be processed as reported above. For a violation to have occurred and be processed, the violation must have involved U.S., foreign government, or international organization classified material, which classification is recognized by the U.S. Government, and it must be an infraction of these regulations.

Adjudication of all security violations is accomplished by the Office of Security. In the adjudication of violations, the principle of primary and individual responsibility as defined in section 903 will be used as a guide. However, in certain incidents supervisors may be held responsible for failure to provide effective organizational security procedures, particularly when other than normal conditions cause the interruption of routine security procedures or controls that are not normally the sole responsibility of any individual.

995.6 Communication Violations

If any violation of the security regulations results in the loss, theft, or unauthorized viewing of cryptographic material or the transmission of an unencrypted classified telegram by an exposed communication channel, a report must be made immediately. Posts should report violations by telegram to the Office of Communications (A/OC), Department of State, with a copy to A/SY/OPS/DO. In the domestic, violations should be reported by telephone to A/OC. (See section 965 for reporting missing or compromised COMSEC material.)

995.7 Disciplinary Action for Security Violations in State, AID, USIA, ACDA, and OPIC

a. After an affirmative adjudication of a violation, one of the following actions may be taken under applicable personnel rules and regulations:

(1) Letter of Warning;
(2) Letter of Reprimand;
(3) Suspension without pay; or
(4) Dismissal.

b. Violations are counted toward disciplinary action for 2 years from the date of occurrence. The Office of Security issues warning letters to employees having no more than two violations occurring in the same 2-year series of violations. In the case of an employee charged with three or more violations in any 2-year series, the Office of Security will recommend appropriate disciplinary action to the Office of the Director General. The Offices of Security at AID and USIA submit such recommendations to their respective Directors, Office of Personnel Management. In OPIC, disciplinary actions will be referred to the President. Extraordinary violations are dealt with on an individual basis. Should circumstances warrant, the agency may take action under the provisions of section 5-503 of the Order and Executive Order 10450.

c. Criteria for administrative action include:

(1) First Violation: Begins a 2-year period for violations. A letter calls the violator's attention to the need to be more careful, and the possible disciplinary action that could result from future violations in the 2-year period.

(2) Second Violation: When occurring in same 2-year series of violations, a letter of warning advising of criteria and penalties for future violations before cut-off date.

(3) Third Violation: When occurring in same 2-year series of violations, a recommendation for Letter of Reprimand to Director General of the Foreign Service or, in AID, to Director, Office Personnel Management.

(4) Fourth and additional violations: When occurring in same 2-year series of violations, a recommendation for suspension without pay is sent to the Director General of the Foreign Service or, in AID, to Director, Office of Personnel Management.

(5) After 2 years have elapsed since the previous first violation, a subsequent violation starts a new 2-year period and the routine letter regarding disciplinary action is repeated.

It should be noted that the Office of Security reserves the right to recommend disciplinary action at any time should the seriousness of the violation warrant such action.

d. USIA records include:

(1) Reports of first violations which result in Letters of Warning to an employee are retained by the Office of Security, USIA, in a pending file and are destroyed after 2 calendar years if a second violation is not charged within that period.

(2) Records of disciplinary action taken by the Director of Personnel are retained in the employee's Official Security and Personnel files, normally for a period of 3 years, and then destroyed as no longer timely or relevant.

995.8 Infractions Involving Administratively Controlled Material

a. Material designated with administratively controlled markings, such as Limited Official Use (LOU), is not classified material as defined in the Order. The failure to secure such material cannot be considered a security violation, however, this material must be protected as required by 5 FAM 958 and the Office of Security will use its resources to insure that such material is properly protected.

b. Security officers will make appropriate inquiries to determine if unauthorized persons have had access to controlled material and to ascertain responsibility when a violation occurs. Reports of Violation (OF-118), will be processed in the same manner as violations involving classified material, but the Report of Violation will be retained at post and not forwarded to A/SY/OPS/DO, except in the case of violations involving AID.

996 CRIMINAL LAWS

Criminal statutes establishing penalties of fine and imprisonment for the release of information in violation of such statutes are set forth in Appendix IV.

997 through 999 (Unassigned)

"Security Regulations : Policy and Procedural Implementation of E.O. 12356
Foreign Affairs Manual Vol. 5" の骨子仮訳
(米国国務省, USAID, USIA, ACDA, OPIC の共用マニュアル第5巻 国家安全保障関係情報の取扱について)

安全保障規則 第900章

各職員に下記の事項を要請する。

a. 本マニュアルの規則に習熟し, かつこれを守る。

b. 常に最新版を保持し, かつ容易に参照できるようにしておく。

c. 差し換えのすんだ古い版を破棄する。

910 政策と手続上の安全保障

911 一般政策

大統領命令第12356(以下"大統領命令"という)では, 国民は政府の活動に関して知る権利があるが, アメリカ合衆国とその国民の権益のため, 国防と外交関係の特定情報は, 公認されない開示に対して保護されるべきことを規定している。このため大統領命令は国家安全保障に関する情報を秘扱指定したり, あるいは秘扱指定を解除したり, 保護したりするための統一的方式を定めている。

本件マニュアル中の規則は大統領命令及び情報保全監視局(Information Security Oversight Office 以下"ISOO"という。)指令第1号(以下"ISOO指令"という。)の実施の促進のため定められた。本件マニュアルの利用者は, 同時に大統領命令及びISOO指令を参照することができる。

秘扱情報の自動化情報システム保安担当者は, 本件マニュアルの他, 別途定めるマニュアル, 基準を参照のこと。

912 実施と監視責任

大統領命令は, 秘扱情報を創出あるいは取扱う官庁は各々, 大統領命令の実施細則を定めるべきこと, また情報保全計画を指揮管理する上席担当官を指名することを規定している。この上席担当官は下記の責任を負う。

a. 秘扱情報を適正に保護し, また保護を必要としなくなった情報を秩序正しく秘扱解除し, また秘扱区分指定が過度に高目あるいは低目にならないよう指導・監視する。

b. 秘扱情報のうち, 議会にも国民にもかかわりがある例外的な性格を有する情報の開示について検

討する。

c．秘扱指定及び解除のガイドラインを作成する。

(1) 当該官庁の長官に以下の勧告を行う。

(2) 大統領命令第1.6節(c)に基づく秘扱再指定のための建議。

(3) 大統領命令第1.3節(a)(0)により保護を要するもの。

(4) 大統領命令第1.5節(b)に定められた表示要件の免除。

(5) 大統領命令第2.2節(c)に定められた手引書作成要件の免除。

d．機密（Top Secret），極秘（Secret），秘（Confidential）の類別による指定権限を委任された担当官の氏名，役職名リストの作成。

e．情報保全計画の管理。

f．公認されない開示又は秘扱解除拒否等異常重大事態下での矯正的又は懲戒的指導。

g．ＩＳＯＯ局長との連絡。

912.1 国務省

国務省の本件上席担当官は秘扱指定／秘扱解除センター担当の次官補（ＤＡＳ／ＣＤＣ）である。

912.2 ＡＩＤ（国際開発庁）

ＡＩＤの本件上席担当官は検査監（Inspector General）である。

912.3 ～ 912.5 略

913 秘扱情報保全責任

913.1 一次責任

秘扱情報保全の責任は，入手方法を問わず，その情報を知識として把握し，物的保管を行っている各個人に在る。

913.2 個別責任

職員各々が本件規則の全てに習熟し，これを遵守する責任を有する。

913.3 監督責任

秘扱情報保全の究極の責任は監督の地位に在る者にかかっている。監督者は秘扱資料が本件マニュアルの規則に定める手続きによって取扱われていることを確認すると共に，部下が通常の義務以上に不当に情報の保全責任を課せられていないことをも確認しなければならない。

913.4 組織上の責任

国務省，ＡＩＤ共に保安局（Office of Security）が各々の機関の物的，手続き上及び人的保全の責任を有す。国務省の通信の保安責任は通信保安部（ＣＯＭＳＥＣ）が負う。

914 ～ 919 （未定）

920　秘扱指定

921　一般政策

a．情報を秘扱にする必要性について妥当な疑義が生じた場合，関係情報は，秘扱指定担当当局が結論を出すまでは，一応秘扱として保全する。秘扱のレベルについて妥当な疑義が生じた場合，関係情報は秘扱指定担当当局が結論を出すまでは，当初の格付よりも一段高いレベルで保全する。

b．情報は，その開示が国家安全保障に不利益な結果を招くと予想されない限り，秘扱指定してはならない。また情報は，法律違反，非効率，行政ミスを隠すため，個人，組織体，官庁への迷惑を防ぐため，競争を抑制するため，国家安全保障上保護する必要のない情報の公開を妨げたり，遅らせるために秘扱指定してはならない。

c．大統領，省庁長官，または秘扱指定権限を委任された官僚は，下記のとおり書面による決定のある場合，以前に秘扱指定解除され，開示された情報であっても，再度秘扱指定ができる。

(1)　国の安全保障上情報を保護する必要があるとき。

(2)　情報が適度にその価値を取り戻したとき。

以上の秘扱再指定措置はＩＳＯＯ局長宛直ちに報告を行うものとする。

d．秘扱指定は適正に行うべきこと。

また特定文書について秘扱指定あるいは秘扱再指定を行うときは，文書の所有者全てにその旨通知するものとし，国務省では指定／再指定決定メモのコピーを外務情報管理センター（ＦＡＩＭ）に送付するものとし，またこの指定／再指定決定がＤＡＳ／ＣＤＣ以外の部局で行われた場合は，当該部局から関連メモのコピーをＤＡＳ／ＣＤＣに送付するものとする。

e．略

f．ＡＩＤにあっては秘扱指定／再指定は長官，及び人事・総務担当副長官の責任において行う。

g．h．略

i．秘扱指定された情報は，同一又は同様の情報が米国内又は国外において非公式に，あるいは不注意から不当に開示されたとしても，自動的に秘扱指定解除にはならない。

922　秘扱区分指定

922.1　秘扱区分の指定

正当な秘扱区分は以下の３種のみとする。

Top Secret（機密），Secret（極秘），Confidential（秘）である。

922.1－1　Top Secret（機密）

情報の不当な開示により，国家安全保障が極めて重大な損害をこうむることが当然に予想される場合，当該情報は“機密”に区分される。この“機密”の区分指定は最も慎重に（with utmost restraint）行わなければならない。

“極めて重大な損害”の例としては，合衆国又は同盟国に対する武力敵対行動，国家安全保障に本質的悪影響を与える外交関係の断絶，重大な国防計画又は複雑な秘密情報組織の危機，秘密情報収集活動の暴露，国家安全保障に不可欠な科学技術開発の内容の開示が挙げられる。

922.1－2 Secret（極秘）

情報の不当な開示により，国家安全保障が深刻な損害を受けると予想される場合，当該情報は“極秘”に区分される。この“極秘”の区分指定は控え目に（sparingly）しなければならない。

“深刻な損害”の例としては，国家安全保障に重大な支障を与える外交関係の断絶，国家安全保障関係の計画あるいは政策の価値の減損，重要な軍事計画又は情報活動の暴露，国家安全保障に関する科学技術開発内容の開示が挙げられる。

922.1－3 Confidential（秘）

情報の不当な開示により，国家安全保障が損害を受けると予想される場合，当該情報は“秘”に区分される。

法律による別段の定めがない限り，秘扱指定された情報の識別には他の用語は一切使用してはならない。例えば“For Official Use Only”とか“Limited Official Use”といった用語は国家安全保障関係情報を識別するのに用いてはならない。これに関連し，“Secret Sensitive”あるいは“Agency Confidential”の用語も使用してはならない。

922.2 外国政府の情報

外国政府によって秘扱指定されている情報の場合，そのまま原秘扱レベルを持続するか又は，情報提供主体の要求するレベルと同等程度の保護を確保できる米国の秘扱区分を指定するものとする。外国政府によって情報が特定の秘扱区分がされていない場合，情報内容がどの程度の注意を要するかによって，かつ，その不当な開示が国家安全保障に及ぼすと予想される損害の程度によって，適宜の秘扱区分を指定するものとする。

923 秘扱指定の要件

本マニュアル中の諸規則が，国務省，ＡＩＤ等５官庁における情報の秘扱指定のための唯一の根拠である。

この秘扱指定の実行には以下２つの要件（ａ．及びｂ.）を満たす必要がある。

ａ．先ず下記の基準の１つを取扱うものであること。

(1) 軍事計画，兵器，作戦

(2) 国家安全保障に関する組織，設備，構想，又は計画の弱点あるいは能力

(3) 外国政府の情報

(4) （特務活動を含む）諜報活動，その情報源及び情報入手方法

(5) 米国の外交関係又は対外活動

(6) 国家安全保障関連の科学，技術，経済的事項

(7) 核物資と施設とを保護する米国政府の計画

(8) 暗号

(9) 秘密情報源

(10) 秘扱指定権限を委任された官僚が秘扱指定した上記以外の部類の諸情報。この項に基きなされた決定は直ちにＩＳＯＯ長官に報告すること。

b．次に秘扱指定権限を委任された官僚は，当該情報の不当な開示が国家安全保障に損害を及ぼすものと予期できることを判定し，決定すること。

c．特に単独では秘扱指定されずに置かれる情報であっても，他の秘扱情報あるいは秘扱されていない情報との組合せによっては，秘扱を必要とする場合は，秘扱指定を行うものとする。

この基準に基く秘扱指定は，書面にてその理由を明らかにし，その情報のファイル又は記録コピーにその理由説明書を添付しておくことを要す。

924 秘扱指定権限

a．国務省では，情報を機密（Top Secret）として最初に区分指定できる権限は長官がこれを有す他，かかる権限を職務上頻繁に行使しなければならないＤＡＳ／ＣＤＣや権限を委任された担当官もこれを有すが，通常次官補（Deputy Assistant Secretary）以下であってはならない。海外においては公館長及びこれに次ぐ者がこの権限を有す。

b．情報を極秘（Secret）として最初に区分指定できる権限は，機密指定権限保有者の他，ＡＩＤ長官がこれを有す。極秘指定権限保有者はこの権限を下僚に委任することができるが，通常，局長（在外公館では各部の長），国別広報官（Country Public Affairs Officers）以下であってはならない。

c．情報を秘（Confidential）として区分指定できる権限は，機密及び極秘指定権限保有者がこれを有すが，この権限を下僚に委任することができる。

d．どのレベルにおいても委任された秘扱指定権限を更に下部に再委任してはならない。

e．指定権者不在の場合は，不在中の代行を委任された者が指定権限を行使する。

国務省にあっては秘扱指定／秘扱解除センター，ＡＩＤにあっては保安担当官（Security Officer）が区分別に，秘扱区分指定を行う担当官の職位リストを保管する。

925 秘扱指定基準

925.1 秘扱文書の参照文を以って，秘扱指定の基準として使用してはならない。（文書本体の内容で秘扱指定の可否を判断すべきこと。）

925.2 秘扱持続期間

a．秘扱期間は必要なだけの期間とし，秘扱指定時に，合わせて解除予定期日あるいは解除要件を設定する。

b．自動的に秘扱解除される仕組になっていない情報，また解除前に審査をするよう定められた情報は，審査が終了するまでは元の秘扱のまま据置く。

c．前任の秘扱指定権者の命令に基く秘扱自動解除は，権限ある担当官による秘扱延長決定がない限り，そのまま有効である。延長の場合はその事実を当該情報の保持者に速かに通知する。

925.3　派生的秘扱

a．秘扱指定された文書に関連し，派生的に秘扱指定する個人は，必ずしも本来の指定権者でなくてもよい。

b．派生的秘扱指定を行う者は，原秘扱指定を尊重しなければならない。派生文書が言い換え，抜すい，削除等により当初の秘扱指定根拠が明確に失われた場合にのみ，秘扱指定が取り除かれたり，秘扱のレベルを引下げたりできる。

c．略

d．当初秘扱指定権限を有する諸省庁は，派生的秘扱指定を容易，適正，一律的に実施できるよう秘扱指定手引書を作成する。

e．略

f．秘扱指定手引書は少くとも２年毎に見直しを行い，必要に応じ更新する。各省庁は手引書一覧表を保管する。

g．各省庁長官は正当な理由のある場合は，手引書作成のための要件を放棄したり撤回したりできる。この場合ＩＳＯＯ長官は通知を受けるものとする。

926　秘扱指定解除　全般

926.1　省庁間調整

国家安全保障に対する配慮により許される限り，情報の秘扱指定はできる限り早期に解除されるか，レベルを下げられるべきである。

この見直しのため各省庁は他省庁及び外国政府との間で連絡に努めるものとする。

926.2　秘扱指定の解除あるいは格下げを行う権限

a．秘扱指定の解除あるいは格下げを行う権限は，当初秘扱指定を決定し，なお同一地位に留まっている担当官，あるいはその後任者，あるいは当該省庁長官により文書でこの権限を委任された者にあり，これらのいずれかによって実行される。

ＩＳＯＯ長官は情報が大統領命令に違反して秘扱指定されていると判断した場合は，当該省庁に秘扱指定解除を要求でき，またこれに対し各省庁は国家安全保障会議に提訴できる。当該情報は提訴に対する結論が出るまで秘扱指定のまま据置かれる。

b．各省庁は上記解除，格下げ権限保有者の一覧表を保持する。

926.3　秘扱指定解除のための系統的審査

a．各省庁は歴史的価値のある秘扱指定の記録を一覧表に取りまとめ，自身で解除のための審査を行

うか，秘扱指定解除指針と共に当該記録を米国公文書館に回付し，その審査を求めるかのいずれかを選択できる。

b．～i．略

j．各省庁は秘扱指定解除の審査に際し，国防長官及び中央情報局（ＣＩＡ）長官各々が発出した，諜報活動（特務活動を含む）に関連する記録の秘扱指定解除審査用の特別手続きに規制される。

927　強制的審査

各省庁は，以下（ａ．～ｃ．）の場合に，下記ｄ．に掲げた場合を除き，大統領命令の強制的審査条項に従って，秘扱指定解除のための審査を行う。

a．米国国民，在留外人，連邦政府機関，州政府，地方自治体から請求があったとき。

b．その請求において，各省庁の適正な努力により当該情報を検索し得るよう，明確に情報資料を説明しているとき。

c．請求を受ける省庁が，当該情報の出所であるとき。

d．外国政府の情報

(1)　外国政府情報の秘扱指定を解除する際は，当該情報を最初に受入れ，あるいは秘扱指定した機関が，解除決定の責任を有す。最終決定に先立ち，適切な経路を通じて外国の情報源と協議を行うことが必要と思われる。

(2)　請求を受けた情報につき全てを秘扱指定解除できない場合は，解除できない部分を除き，公開できるよう適度の努力を行うものとする。

開示請求を拒否する場合は，請求者に対し拒否回答受理後60日以内を条件に不服申し立てをする権利があることを通知し，申し立て処理手続規則のコピーを１部同封する。

e．情報開示請求に対して，検討に時間がかかる場合であっても，異例の状況にある場合を除き，受理から１カ年以内に最終決定を下すものとする。

f．大統領命令第3.4節b)に同じ。

g．略

h．最近，審査を行い，開示を拒否した資料に対するいかなる請求も，これが当初の拒否に対する不服申し立てを構成しない限り，再度これを審査せず却下して差しつかえない。

i．略

j．情報公開法，プライバシー保護法，大統領命令に定めるところにより，請求された情報の存在自体が秘扱指定すべき事項である場合は，その存在あるいは不存在の確認や否認を行うことを拒否するものとする。

k．不服申し立ての内部処理細則は以下を参照のこと。

(1)　国務省　５ＦＡＭ900，22ＣＦＲ　第171．22節及び第171．60節

(2)　ＡＩＤ　ＡＩＤハンドブック18，　パートⅢ，第11章

以下略

928　手数料料率表

国務省　22ＣＦＲ　第171.5節，第171.13節参照

ＡＩＤ　22ＣＦＲ　212/35参照

929　大統領により任命された者（Presidential appointee）によるアクセス処理手続

国務省　22ＣＦＲ　第171.25節参照

ＡＩＤ　22ＣＦＲ　第171.25節参照

930　文書の区分表示（marking）

931　識別と表示

大統領命令第1.5節(a)に定める表示は文書以外の材料にも付すものとする。

秘扱指定レベルを表示するため“Top Secret”（機密），“Secret”（極秘），“Confidential”（秘）の表示（マーキング）を付す。

931.1　全面表示

文書への表示は，情報の本文から明白に区分できるやり方で，かつ当該文書中の情報の最高の秘扱区分を表示する。

このマーキングは，（もし表紙があれば）表紙の外側の上及び下に，（もしタイトル・ページがあれば）タイトル・ページに，第1ページに，及び（もし裏表紙があれば）裏表紙の外側に表示するものとする。

931.2　ページ・マーキング

秘扱指定された文書の各ページの上部及び下部には，当該ページ中の情報の最高の秘扱区分（当該ページ中の情報が全て秘扱でない場合は一般：“UNCLASSIFIED”と表示する。）を表示するか，もしこれが余りにも煩雑であれば，上記全面表示と同じ秘扱区分をやはり各ページの上部及び下部に表示する。

931.3　部分別マーキング

特定文書又は情報について，部分（portion）ごとに秘扱区分を表示するものとするが，かかる文書又は情報の利用，流通がほとんど見込めず，また行政上の負担が部分別マーキングのメリットを上回るとの理由があれば，各省庁長官は部分別マーキングの要件を放棄できる。

この要件を放棄しない限り，文書の各部分（タイトルや主題も含め）には，本文の直前，直後のどちらかに，カッコで表示した記号，すなわち機密は“（ＴＳ）”，極秘は“（Ｓ）”，秘は“（Ｃ）”，一般は“（Ｕ）”の記号を表示する。これらの記号の適用が実際に即さない場合は，それに代る充分な

説明が記載されることを要す。

文書の全部分が同一基準で区分されている場合には，その旨の説明により表示してもよい。例えば“Confidential－Entire Text”（全文とも秘）という具合である。

(1) 国務省では下記文書の部分別マーキングの要件を既に放棄してある。

(a) 機密（Top Secret）情報を内容とする文書

(b) 次官（Assistant Secretary）級以上用に作成された行動／情報の覚書

(c) 在外公館への指示及び交渉の権限委任に関する指示

(d) 省内の調査研究

(e) 省庁間及び省内での覚書

(2) 国務長官はまた，外国政府の情報を含む文書については，電文であれ非電文であれ，部分別マーキングの要件を放棄してある。

931.4 表示の省略

前任者により指定された秘扱区分の表示が省略されていても，然るべき基準で秘扱指定されているとみなすものとする。省略されている表示は，指定権者によりあらためて挿入できる。

931.4－1 秘扱指定権限

文書の署名者又は決裁者とは別の者が秘扱指定した場合は，“○○によって秘扱指定済み”“CLASSIFIED BY（“表示権者あるいは当初の秘扱指定権者”）”と表示する。

931.4－2 起源としての省庁，事業所

情報・文書の起源となっている官庁等の識別が文書の文面上明示されていない場合は，前項の“CLASSIFIED BY……”の行の下にこの表示を行うものとする。

931.4－3 秘扱指定解除及び格下げの指示

a．特定期日又はでき事に際し自動的に秘扱指定解除される情報については“DECLASSIFY ON（日付）”または“DECLASSIFY ON（でき事の記述）”と表示する。

b．自動的には解除されない情報については，“DECLASSIFY ON：Originating Agency Determination Required”又は“DECLASSIFY ON OADR”（秘扱指定解除には起源官庁による決定を要す）と表示する。

c．特定期日またはでき事の発生に際し自動的に秘扱レベルの格下げが行われる情報については“DOWNGRADE TO（秘扱区分レベル）ON（日付又はでき事の記述）”と表示する。

931.4－4 特殊表示

a．送達用文書

送達用文書はその表書きにその文書が送達する情報の最高秘扱区分を表示する。また以下の指示かそれと同様の指示を表示する。

(1) 一般扱の送達用文書には，“UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED”（秘扱指定の同封物が除去された時は一般扱）

(2) 秘扱指定の送達用文書には，“UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS（以下送達用文書のみの秘扱区分）”（添付物件の除去と同時に本文書は…）と表示する。

b．原子力関係データ （略）

c．諜報情報収集源及び方法

諜報活動関係の情報収集源又はその方法に関する文書には，他に中央情報局（CIA）長官による定めのない限り，下記表示を行う。

“WARNING NOTICE－INTELLIGENCE SOURCES OR METHODS INVOLVED”（注意－諜報情報収集源あるいは方法を取扱）

d．外国政府情報（FGI）

外国政府情報を内容とする文書には，“FOREIGN GOVERNMENT INFORMATION”の表示を行う。

情報がFGIであることを秘す必要のある場合は，この表示をせず，米国起源の情報であるかの如き表示を行うものとする。

931.5 電送情報（通信文，電報）

電送される国家安全保障関係情報の取扱は，

a．当該情報の最高の秘扱区分表示を本文第1行目の前に行う。

b．“CLASSIFIED BY……”の行は不要。

c．秘扱指定存続期間は次のとおり表示。

(1) 特定期日又はでき事に際し，自動的に秘扱解除となる情報については，“DECL（日付）”又は“DECL（でき事の記述）”と略号表示。

(2) 自動的に解除されることなく，起源官庁の決定を必要とする情報については，“DECL：OADR”と略号表示。

(3) 自動的に秘扱指定区分が格下げされる情報については，“DNG（日付またはでき事の記述）”

d．部分別マーキングは前述のとおり。

e．(1) 原子力関係 （略）

(2) 諜報情報関係については別段の定めのない限り“WNINTEL”と略号表示する。

(3) 外国政府情報はFGIと略号表示。

FGIであることを秘匿する必要のある場合は，この表示をせず，米国起源の情報であるかの如き表示をする。

931.6 秘扱指定区分表示の変更

秘扱指定された情報の区分またはその存続期間に変更があった場合，記録の保持者全員にその旨速かに通知を行うものとし，保持者はその変更根拠を引用しつつ，表示を修正する。一つ一つの情報の表示変更が不当に煩雑となる場合には，変更通知を保管ユニットに取付けるものとする。

932　移管資料

a．単なる保管の目的のみでなく他省庁に主管変更した情報の場合，受理側の省庁がその情報の起源官庁となる。

b．秘扱指定された情報が，その当初の起源官庁が存立を既に終了し，後継機関もない場合，かかる情報を所有している官庁が起源官庁と見なされ，秘扱指定解除または区分指定の格下げは，その情報の所有官庁が，その情報の主題に関心を有する他官庁と協議の上，実施する。

c．米国公文書館に移管した秘扱資料は，大統領命令，ＩＳＯＯ指示書，及び各省庁の指針に従って，アメリカ合衆国文書管理官の手で秘扱指定解除又は秘扱指定区分格下げが行われる。

933　文書の秘扱指定状況表示

933.1　全面表示とページ・マーキング

前述931.1～931.2 に同じ。これは製本されたもの，印刷されたもの，あるいは複写されたもの如何を問わず一律に適用する。

933.2　起案文（working draft）

起案文には妥当な秘扱指定表示を記入すること。最終案決定後その写しを保存する場合は，案文には最終写に示される全ての表示を入れるものとする。

933.3　一般扱資料

通常一般扱資料には“Unclassified”（一般扱）という表示やスタンプ押印は行わないが，当初当該資料を秘扱指定する意図を有していたものの，検討の結果，一般扱とすることが決定されたという事情を知らせる意味であえて“Unclassified”と表示することがある。

934　文書集合体（Groups of Documents）に対する表示

934.1　送達文書

基本的な送達文書に添付物が付けられる場合，送達文書の表面に，添付物の区分表示も目立つように表示する。例えば，秘扱文書を添付物として，一般扱の送達文書と合わせ送る場合には，次のように表示する。

“SECRET（TOP SECRET or CONFIDENTIAL），Unclassified When Separated From Attachment”“極秘（機密あるいは秘），ただし添付書から分離すると一般扱”

934.2　連結された文書（Physically Connected Documents）

ファイル又は集合化された連結文書に指定される秘扱区分は，その中で最高に格付けされた秘扱文書と同一レベルとする。ファイルから分離された文書は各々別個に指定された秘扱区分に応じて取扱われる。秘扱のファイルの表紙（cover sheet）には当該ファイル中の最高秘扱区分を表示する。あるいはフォールダー（folder）の場合は，表紙と裏とに表示あるいはスタンプ押印を行う。

934.3　大量の資料についての取扱

大量の資料について区分表示の変更等の処置を個別に行うことが困難な場合，変更通知は当該資料の保管箇所（ storage unit ）に対して行うことができる。個別の文書，資料等がかかる保管箇所より取り出され，使用に供される場合は，その変更に伴う区分表示修正を然るべく行うものとする。

935　特殊資料への表示

紙製以外の秘扱指定資料への区分表示は，かかる資料の収納物件上にスタンプ押印，印刷，手書き，ペンキ，荷札，ステッカー等により目立つよう行う。このやり方が実際的でない場合は，当該資料の受領者に対し，その取扱を記した書面の通知を届けるものとする。

935.1　図表，地図，図面

図表，地図，図面には汎例，標題，縮尺等の下に区分表示をする。これら資料の全体的区分指定と汎例や標題自体の区分指定が異なる場合は，高い方の区分が各資料の上部と下部に表示される。たたんだり，巻きくるめたりして区分表示が見えなくなる場合は，たたんだり，巻いたりした状態でもはっきり見えるよう追加表示を行う。

935.2　写真，フィルム，録音・録画テープ

935.2－1　写真

ネガ，ポジ両方共区分指定を表示し，目立つ表示をした格納容器中に保管する。

ネガ・ロールにはロールの両端に表示をし，一枚づつのネガには各々表示を行う。

写真プリント一枚づつにも表面の上部と下部に表示をし，かつ裏面の中央にも表示をする。

自動現像方式のフィルムあるいは印画紙を使用する場合，使用後の関係材料を秘扱廃棄物として破棄するか，あるいはカメラ自体を秘扱資料としてそのまま保護する。

935.2－2　ＯＨＰ用透明紙及びスライド

ＯＨＰ用透明紙，スライドには一枚ごとに表示を行い，可能ならば縁，ホールダー（ holder ），枠等にも表示する。

935.2－3　映画フィルム

秘扱指定の映画フィルムは各リールの頭と終りに表示し，また映写時には表示が見えるようにしなければならない。リールの容器にも目立つ表示をすること。

935.2－4　録音・録画テープ

録音・録画テープには両端末に，いかなる視聴者にも当該テープの一部があるレベルの秘扱指定されていることがわかるよう説明を入れる。テープは目立つ表示を施した容器に入れるか，同様のリールで保管する。

935.2－5　マイクロフォーム（ microforms ）

マイクロフォームは極小画像であり，それ自体は肉眼では認識困難であるが，表示が肉眼で読み取れるようマイクロフォームの素材又はその容器に表示を行う。この表示は映像上にも現示されるよう

仕組むものとする。

935.3 電算機用パンチカードのデッキ（Decks of Accounting Machine Punched Cards）

電算機用パンチカードのデッキも文書の一単位と見なされ，最初と最後のカードに秘扱区分表示を行うものとする。

935.4 移動式自動データ処理及びワープロ用保存媒体

自動データ処理（ＡＤＰ）システム，タイプライター，ワードプロセシングシステムを使用した移動式自動データ処理保存媒体は，その媒体あるいは媒体内の情報を利用する者が，その中の情報が秘扱指定されていることを確実に知り得るよう，外見上も，また内面的にも表示を行うものとする。

磁気式保存媒体が秘扱情報の処理用に使用されると，承認された方法により磁気を解かれるまで，秘扱指定されたままで常に処理され，保護される。詳細については別途定めるSystems Security Standard を参照のこと。

935.5 取外し不能のデータ及びプログラムの保存媒体

取外し不能のデータ及びプログラムの保存媒体は承認された方法にて秘扱指定を解除されない限り，当初の秘扱指定のまま取扱われる。

935.6 ＡＤＰ設備を利用して作成される文書

ＡＤＰ設備利用による文書にあっては，少くとも最初の頁，及び，もしあれば表紙と裏表紙に，全体としての表示を表わす。

内部の個別の頁の区分表示はＡＤＰ設備又は他の手段によって行ってよいが，表示内容の変更を個別頁ごとに行うことが困難な場合は，当該文書の第１頁に“表示変更の指示とその他関連表示”としてスーパーインポーズしてよい。

935.7 研修用教材

秘扱指定文書の取扱研修の一環として，一般扱資料を秘扱資料と見せかけて使用する場合は，当該文書ないしは教材には“（insert classification designation）for training，otherwise Unclassified”（一般扱，ただし研修用としてのみ秘扱指定）と表示する。

936 ～ 937 （未定）

940 秘扱指定情報・資料へのアクセス

941アクセスの一般要件

何人であっても，その者が信頼できると判定され，かつ公的義務を果すために必要と判定されない限り，秘扱情報へのアクセスは認められない。このアクセスは下記に定めるところにより許可される。

941.1 信頼性の判定

何人もその信頼性について好ましい判定が下されない限り，秘扱指定情報へのアクセスは認められ

ない。この適格性の判定基準は当該省庁ごとの基準や規格に基く。原子力関係データ，ＮＡＴＯ情報，暗号，諜報，その他法律により特別の保護が与えられている情報へのアクセスには極めて特殊，特別な許可が必要となっている。

941.2 知る必要（Need－to－Know ）についての判定

いかなる個人も公務上の地位ないし許可を与えられたことのみを以って秘扱情報を受領する権利はなく，公務上の義務の覆行の必要性に関連して求めたり，その他本規則により特に認められる通りのアクセスの必要性に基き求めるものでなければならない。

その必要性の判定は当該秘扱情報に責任を負う担当官により行われるものとする。

942 歴史研究家及び大統領経験者の指定人によるアクセス

a．特定期間における官庁の記録が秘扱指定を解除されている時，これらは米国公文書館に移管されており，これら資料へのアクセスは米国公文書館に取扱いを一任している。

b．国務省は，過去の米国大統領から任命された者が，その在任中に制定，審査，署名，受領した往時の文書へのアクセスを申請する場合，下記全ての条件を満足できる場合に限りこれを許可している。

(1) アクセスの許可が国家安全保障という国益に合致し，かつ申請者が信頼を置ける者との判定が下されていること。アクセスできる情報は，当該官庁が秘扱指定権限を有する範囲のものに限定される。

(2) 申請者が，情報が不当に開示されるのを適用可能な法令により防止できる旨書面で同意すること。

(3) 申請者が，申請者の書く原稿や控えの中に秘扱情報が含まれていないことを確認するための審査を当該官庁に委任することを書面により同意すること。

(4) 当該情報が当該官庁による明示の許可なくして他に伝達されないこと。

(5) 申請者から請求された情報が，適度の努力で検索でき，かつ編集できるものであること。それでなければ，別に定めるところにより手数料を徴収する。

(6) 申請者に代ってアクセスを請求する個人又は調査補助員もやはり上記条件の全てを充すこと。

(7) 調査補助員が編集した情報もまた上記に明示した諸条件の全てに従うこと。

(8) 申請者の指定した情報は，請求があれば，本規則に従って秘扱指定解除のための審査が受けられること。

943 行政部門以外の者によるアクセス

議会に対しては，秘扱指定情報は関係部局間で協議・調整の上，開示される。それ以外には，通常は秘扱指定情報は行政部門以外の者には開示されない。

944　請負業者又はコンサルタントによるアクセス

協定により，国防長官は産業安全保障業務を国務省，ＵＳＩＡ，ＯＰＩＣ及びＡＩＤに代って行う権限を認められている。保安局は秘扱の請負契約あるいは購買発注に参入している請負業者の会社及び従業員の検証を行う。秘扱請負契約の履行に必要な手続を要約した小冊子は保安局で入手できる。

省庁職員は，秘扱指定資料をコンサルタント又は請負業者に公開する以前に保安局の承認を自身で得ておく必要がある。正規職員でない者による秘扱資料保管のための要件については第971.4　節を参照のこと。

945　外国人職員によるアクセス

秘扱指定情報は外国人職員にはその利用に供することも，その保管に委ねることも行ってはならない。外国人職員は特に保安局が承認した場合を除き，秘扱情報が討議される会議に出席することは許可されないものとする。

秘扱情報は外国人職員により聞き取り筆記又はタイプされてはならない。秘扱指定決定手続に外国人職員を文書作成等で関係させてもいけない。ただし，保証されている場合には，外国人職員が収集したり，報告書の形式に作成した情報はそのまま秘扱指定できる。

国家安全保障に関する情報は，ワードプロセッサ・システムやデータ処理装置等外国人がアクセスできる設備に入力してはならない。

946　制限付きアクセスの認可

外国人職員が特権として認められた情報源から情報を入手する，あるいは行政管理上の統制を当然受けられる情報を開発する，あるいはその公務を遂行するために他のどこかを出所とする行政管理上の統制を受けた情報へアクセスする必要がある等の場合，以下の条件で，かかる情報への制限付きアクセスが認められる。

a．外国人職員を管理する米国市民権を有する監督者が，当該外国人職員の公務遂行上の必要性のため行政管理上の統制を受けた情報へのアクセスが必要な理由を明記し，かつアクセスしようとする情報の部類を記述し，書面によってアクセスの許可を請求する。

b．地域別保安対策担当官がその請求を審査し，同意する場合は，情報保安担当上席担当官に制限付きアクセス許可勧告を覚え書にして発出する。

c．上席担当官がこれを認可する。

d．上記アクセスは行政管理上の統制を受けた情報を受領するための総括的な認可によるものと解釈しない。上記a．に明記した種類の情報に限り，かつ厳密に“知る必要性”を拠りどころとして，外国人職員に制限的なアクセスが許可されるものである。

947 ～ 949　（未定）

950　公的な伝達の統制管理

951　他の政府機関の情報

別の機関で発生した秘扱指定情報は発生源の官庁の同意なしに受入側官庁の外部でやり取りしてはならない。この目的上，国務省，ＵＳＩＡ，ＯＰＩＣ，ＡＣＤＡ及びＡＩＤは各々別個の機関と見なすものとする。かかる承認は書面により行うものとし，承認と交信の記録は発信者がこれを保管する。

952　他機関への流通

秘扱情報は既定の連絡・流通経路を通してのみ他官庁に送付できるものとする。

953　諜報関係情報の流通と利用に関する管理

953.1　諜報文書

諜報関係文書に含まれる情報は，特定の管理表示を付されており，かかる統制管理の制限枠内で取扱われることを要す。諜報文書の統制管理については11ＦＡＭ418を参照のこと。

これら規定に従えない場合は，本規則第995節に定めるごとく，規則違反と見なす。

953.2　諜報情報の配布

“WARNING NOTICE－INTELLIGENCE SOURCES OR METHODS INVOLVED”（前掲931.4－4Ｃ参照）の注意書を付された情報は，情報元の官庁の許可なく配布されてはならない。

国務省を情報源とする諜報情報は，

ＩＮＲ／ＤＯＣ／ＯＩＬ／ＣＳの表示が付される。

953.3　特別アクセスプログラム

大統領命令第4.2節に定められた特別アクセスプログラムの下で管理されている特殊な情報の取扱いについては当該プログラムの特別の手続きに従って行われるものとする。

954　法廷又は他省庁の命令又は請求による配布

a．法廷又は他省庁からの秘扱情報に対する召喚，要求，請求は，いかなるものも全て別途定める規程により取扱うものとする。

b．秘扱情報に関する法廷での証言は召喚に対する応答の手続きに従い，手続の定めるところによって必要とされる承認なくして，法廷その他の官庁において証言してはならない。

事前の許可なくかかる証言を求められた職員は，所要の情報の開示は許可されていないこと，及び特定の情報に対する書面による請求は関係当局の長官宛に送達されるべきことを陳述するものとする。

c．　職員の忠誠心（loyalty）に関する報告書，記録，ファイルは秘として保管され，規則に従

ってのみ要求される以外には開示されない。

955　外国政府に対する配布

955.1　外国政府及び国際機関に対する秘扱情報の配布については11FAM500を参照。

955.2　外国政府及び国際機関に対する秘扱軍事情報の開示請求については，全て国務省　政務軍務局　軍需統轄部長　国家軍事情報開示政策委員宛とする。

955.3　外国政府と国際機関への通信保安情報の開示

国家通信安全保障委員会（ＮＣＳＣ）が通信保安情報の開示を規制する国策を制定しており，この種の開示請求は同委員会の国務省のメンバーである国務省通信担当次官補に回付するものとする。

956　特別配布カテゴリー

956.1　暗号表示

“ＣＲＹＰＴＯ”（暗号）の表示は暗号による資料に付せられ，アクセス，保管，取扱，及び説明上特別の配慮が必要である。本規則第980節にこの件に関する説明がある。

956.2　特別配布略符

956.2－1　ＮＯＤＩＳ

“ＮＯ　ＤＩＳＴＲＩＢＵＴＩＯＮ（ＮＯＤＩＳ）”とは名宛人以外には一切配布を認めないことを意味し，大統領，国務長官，在外公館長間の最高機密の通信文にのみ使用される。

956.2－2　ＥＸＤＩＳ

“ＥＸＣＬＵＳＩＶＥ　ＤＩＳＴＲＩＢＵＴＩＯＮ（ＥＸＤＩＳ）”とは本質上知らなければならない担当官のみに配布されることを意味し，ホワイトハウス，各省長官，次官，在外公館長間の高度に機密の通信文にのみ使用される。

956.2－3　ＬＩＭＤＩＳ

“ＬＩＭＩＴＥＤ　ＤＩＳＴＲＩＢＵＴＩＯＮ（ＬＩＭＤＩＳ）”とは知る必要のある担当官，部局，官庁に厳しく制限された配布を意味し，この略符は通常の取扱注意要件を上回る通信文に使用される。

956.2－4　ＳＴＡＤＩＳ

“ＳＴＡＴＥ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＯＮＬＹ（ＳＴＡＤＩＳ）”

国務省以外の連邦政府機関に当初から配布すると国務省の権益に不利となると思われる場合に用いる。“ＥＸＤＩＳ”や“ＬＩＭＤＩＳ”と併用することができる。

957　個人的使用の規制

957.1　個人的利益

秘扱情報は職員のだれもが個人の利益を目的としては使用できないものとし，かつ個人の日記帳や私用の記録中に記入してはならない。

957.2 会話での制約

秘扱情報についての議論は，その内容を知ることが認められていない者の居合せているところや，その話が聴取されるところではしてはならない。

また秘扱情報は，承認済みの確実な通信回路に由ることが認められている場合を除き，電話又は所内インターフォンを用いて会話の中で議論してはならない。

958 行政管理上の統制を受けた情報

958.1 指 定

国家安全保障に係わる情報ではないが，ある種の取扱いに注意を要する資料というものがある。この種の情報は限定的に配布されることになるが，権限を有する担当官により，ＬＯＵ（Limited Official Use ）と指定され，表示される。かかる資料は，少くとも施錠のできる保管キャビネットの中で秘扱（Confidential ）と同様に取扱われ，伝達され，保管される。

958.2 指定解除

別段の定めがない限り，行政統制された情報は，起源となる日から起算して４年後に自動的にその統制を解除される。４年の期間にわたって保護が必要でなければ，特定の事項の発生，統制されている添付書類の除去，又は４年を起えない妥当な期間の経過等と共に，統制が解除される旨を文書上に明記する。

また４年以上にわたる保護が必要な場合は，自動的解除の適用が除外される旨明記する。

ＬＯＵ指定の資料が情報公開法又はプライバシー保護法の定めるところにより開示請求を受けた場合は，開示の可否が審査され，決定される。

958.3 統制解除の表示

統制指定されている情報は秘扱指定情報に適用されるのと同じやり方でＬＯＵ表示がされる。文書が４年目の時点で自動解除されるものを除いて，解除表示は電信文等の最終行として記入されるか，又はその他の文書では表紙の下方に記入される。

４年を待たずに特定日時，行動又はでき事の終了と同時に解除できる情報は，

" Decontrol on _____ "（_____を以って解除）と表示し，_____には日付，またはでき事の記述を記す。

法令により自動解除の適用から除外される特定の情報や資料には次の表示を行う。

" Exempt from Automatic Decontrl by Statute "

（法令により自動的解除を適用されない）

また法令により自動解除の適用をされなかったり，４年以上の長期にわたって保護を必要とする場合，" Exempt from Automatic Decontrol ; Authorized by _____ "

（自動的解除の適用を除外；_____により承認）

と表示される。

上記例の後者の部類の場合は，情報を秘扱指定できる権限を有する担当官の承認を得て，自動的解除の適用から除外できるものとする。

960 秘扱資料の伝達と管理

961 機密（Top Secret）資料管理要領

961.1 要 件

大統領命令の定めるところにより，機密文書管理官（Top Secret control officer）の任命が必要とされている。機密文書カバーシート，機密文書管理番号，機密文書受領書が，機密文書の理由を説明し，アクセスした個人の識別をし，受渡しを確実にするために有効であり，その使用が定められている。

961.1－1 機密文書管理官の任命

a．海外の場合

海外の職場においては，機密資料の利用，保存，配布に関して運用面の決定を下すことのできる上席担当官が機密文書管理官として任命される。この代理者としては通常，機密資料の保管の必要条件からして，通信と記録部門の監督者がこれに当てられる。

機密文書管理官及び代理者の氏名，役職名，選任日付が記載された文書にて，選任通知が地域別保安担当官に通知される。

b．国内の場合

各関係局局長は，局内の機密資料の保管責任を有する上席担当官を機密文書管理官及びその代理として任命する。この選任された局内機密文書管理官は，保安局の同意を得た上で，局内の部課で業務活動上の必要性又は物理的条件から追加選任が必要となった場合，各単位部門ごとに機密文書管理官を各々任命できる。局内機密文書管理官は，局内機密資料や記録の取扱について第一義的責任を負う。

ＡＩＤにあっては総務局の中に中央機密文書管理官が設けられ，この総括的管理官は各局の機密文書管理官名簿を管理する。

961.1－2 機密文書管理官の義務

a．管轄下の機密文書の厳重管理

b．管轄下の機密文書全ての受領，保存，発行，複写及び破棄

c．管轄下で発生し，または受入られた機密文書の永久登録リストの保管

d．管轄外に出したり，破棄した機密文書の受領書の保持

e．機密文書の区分指定見直し

f．機密文書の破棄あるいは回収の指示

g．年間報告書の作成

海外の機密文書管理官は当該報告書を地域別保安担当官に，ＡＩＤ（ワシントン）の機密文書管理官は本書を中央機密文書管理官に，写しを保安局に提出する。

ｈ、機密文書管理番号の割り付け。

ｉ．機密文書の写しの作成に先立ち，情報発生源の部局の承認取り付け。

ｊ．機密文書取扱が本件規則に従い実施されていることの確認。

ｋ．機密文書へのアクセスを認められた者が，機密文書カバーシートに受領署名をすることの確認。

ｌ．保管期間中の機密文書のチェック（区分指定変更，破棄の可能性を探るため）

ｍ．機密文書の伝達が規則に則り行われていることの確認。

ｎ．自動化情報システム中の機密情報の管理が，規則に従って行われていることの確認。

961.１－３　ＵＳＩＡ　（略）

961.１－４　機密情報の在庫チェック

機密文書管理官は10月31日現在で毎年機密情報の員数調査を実施するものとし，各文書が現存しているのを実証することが絶体に必要（ mandatory ）である。この在庫チェックで一致しないことがあれば，保安局に直ちに（ immediately）報告するものとする。

機密文書管理官はこれら不適切な管理によって生じた，管轄下機密文書の紛失に対して最終的な責任を有す。

961.２　機密文書管理番号

961.２－１　機密文書管理番号の指定

機密文書が生じたり，受入れた場合は，同文書の各写しの上部右上に管理番号を表示する。最終案が配布されたら，草案の写しは破棄しなければならない。草案のまま許可を得る必要があるか又はその他の理由のあるときは，草案写しに一連の指定管理番号及びコピー番号の割り付けを受ける。

961.２－２　機密文書管理番号の構成

機密文書管理表示は，海外駐在先あるいは国内の組織別単位によるものとする。機密文書管理官が次々と交替しても，後任者は前任者の管理表示記号を踏襲する。

ａ．海外駐在先の場合

機密文書管理番号がＬＮＤ－79/18-A/3 とするとＬＮＤはロンドンの略号，79は年号，18は駐在先で発生又は受入のあった18番目の機密文書，Ａはシリーズになっているとの意，３はシリーズでの３番目の複写であることを意味する。

ｂ．省庁内の場合

機密文書管理番号がＥＵＲ－79/38－A/8 とすると，ＥＵＲとはヨーロッパ局の略号，79は年号，38はＥＵＲで発生又は受入のあった38番目の機密文書，ＡはＥＵＲにおける第１番目の複写，８はシリーズでの８番目の複写であることを意味する。

961.２－３　機密管理番号の割り当て

駐在先又は組織単位において，機密文書が生じたり，受入れがある都度，管理番号を割り付け，文

書には機密のカバーシートを添付する。ＡＩＤではこれらの任務は専ら中央機密文書管理官の業務である。

961.2－4　機密文書表紙

機密文書の原本及び各コピーには各々機密文書用表紙でカバーが付される。この表紙は機密文書管理官により整えられるが，管理番号，資料の種別，主題件名，日付，宛先及び創出者が記載される。

機密文書にアクセスできる者は全て，表紙に署名し日付を記入する。

このカバーシートは内容の文書が以下のどれかになるまで文書と一緒に保存される。

a．他省庁に移管されたとき

b．破棄されたとき

c．使用されなくなったとき

d．秘扱区分指定が格下げになったとき

e．秘扱を解除されたとき

上記の措置が１つでも取られた場合は，管理官は表紙にその措置を記録し，５カ年間保存し，その後破棄する。

961.2－5　配　布

機密文書の配布は機密文書管理官又はそれに代る者によって行われる。配布の際受領証がやり取りされ，機密文書受領証は他の秘扱レベルの低い文書の受領証とは別個にファイルされる。

機密文書に責任のある者は，その文書を機密文書管理官の同意を得ずに，別の者に伝達してはならない。

機密文書管理官以外の職員は，管轄部局外から機密文書を直接受領してはならないし，また管轄部局外に伝達してもならない。

961.2－6　行政措置

機密文書を紛失したり，機密文書又はそのいかなる部分をもその起源官庁あるいは部局の許可なくコピーを作成したり，機密情報の内容を“知る必要”のない他の職員に知ることを許したりした職員は，徴戒又は給与支払停止などから成る行政措置による処分を受ける。

本規則の甚だしい軽視は免職又は訴訟にも及ぶことがある。

962　伝達・輸送方法

962.1　認可された経路

秘扱文書を国境を越えて伝達する際は外交クーリエを使用のこと。

962.2　機密文書の伝達

機密文書の伝達は下記のいずれかの手段によらなければならない。

a．機密文書メッセンジャー

b．認可されたクーリエ

c．暗号形式による電気的手段

962.3　極秘文書，秘文書の伝達

極秘及び秘文書も機密文書伝達用に承認された手段のうちの１つを利用すべきであるが，その利用が容易でない場合は，米国書留郵便又は米軍郵便の経路を利用できるものとする。

ただし、いかなる場合も、米国公務員による統制から外れてもならず，かつ外国の郵政組織を通過することもないものとする。

962.4　一般扱資料の伝達

海外駐在先では，一般扱資料の伝達は外交パウチ，米国第１種郵便，又は外国の郵便組織を利用する。

962.5　伝達のための準備

962.5－1　封筒，容器，カバー

a．秘扱指定された文書はカバーを掛けるか，内側に向けて折りまげ、不透明な封筒の中に封入しなければならない。

b．内側の封筒には宛先の担当官の役職名を明記し，封筒の両側に適切な秘扱区分表示を行う。外側の封筒は米国の郵便業務に必要なため，宛先を記入するが，保安上の秘扱区分やその他内容物が秘扱になっている旨のいかなる表示もしないものとする。返信用として発送者の宛先も封筒内に入れておくものとする。

962.5－2　受領書と登録

所定様式による受領書に内容物の区分表示，内容の種別，件名，コピー番号・連続番号，文書の日付等所要事項を記入し，文書の発送者と受領者の間でやりとりされる。

所定要件が満たされない，あるいは受領書が戻ってこない等の事情が解決されなければ，保安担当官に通報しなければならない。

962.5－3　受領書の処理

秘資料のやりとりに係る受領書は，送達・受領の発生日より２年後に破棄してもよい。

962.5－4　外交パウチの利用

外交パウチを利用して送付する際は、別に定めるところにより利用記録が登録される。

962.5－5　磁気利用保存装置の送達

秘扱資料を磁気利用保存装置に入力して他部門、他省庁等に送達する場合、当該資料は磁気式保存装置にコピーしておくものとする。

963　機密資料の複製

963.1　基本方針

秘扱指定情報を内容とする文書を複写することは，危険性を最少限に抑えること，保管コストの低減を図ることのために，必要最少限に抑えることが必要である。

複写が禁止されている場合は、その旨明記する。秘扱資料を許可なく複写することは，相応の懲戒の対象となる。秘扱資料の複写コピーも原本と同一の責任と管理の下に置かれるものとする。

本規定は秘扱指定解除のための審査の目的で当該秘扱文書を複写することを妨げるものではないが，審査の後もそのまま当該文書が秘扱される場合は，審査目的で作成した複写コピーは破棄しなければならない。

963. 2　機密文書の複製

特に明示がない限り，機密文書を複製する許可は，複製を企図する部局の機密文書管理官が，文書起源の部局の機密文書管理官から取得しなければならない。ＡＩＤワシントン本部においては，他に別段の明示がない限り，機密資料の複製には総務局長（ Executive Secretary ）の承認が必要であり，かつこの複製作業はExecutive Secretaryの勤務要員によってのみ実施可能とする。

963. 3　極秘文書，秘文書の複製

a．特に明示がない限り，極秘文書，秘文書の複製は，その文書の起源の部局あるいは省庁の承認を受けなくてもよい。ただし複製は効率的な運営に必須の場合にのみ行うものとする。

b．ＡＩＤワシントン本部においては，秘扱電信の複写は電信課によってのみ可能である。複写の請求は各部局の局長級又はそれと同等の担当官の明示的承認の表示を必要とする。（所定様式使用）

963. 4　複製の記録

複写コピー枚数，配布部数を示すため，全ての省庁は秘扱文書の複写記録を保持するものとする。

963. 5　秘扱資料の複写設備の保護

秘扱資料を複写する設備は一般扱資料の複写とは運用を別にして管理すべきであり，通常の勤務時間中は，身元の明白な米国人職員の定常的監視及び管理の下に置き，勤務時間外は施錠された部屋内に保管しなければならない。

964　秘扱資料の破棄

秘扱資料の破棄は，身元の明白な米国人職員により，承認された手段により，慎重かつ完全に行われるべきこと。

964. 1　機密資料の破棄

964. 1－1　要　件

機密文書管理官は，機密文書カバーの上に当該資料の破棄を記し，その文書カバーを５年間保存しなければならない。

964. 1－2　破棄の立会人

機密文書管理官は，破棄担当官として，破棄指示書に署名し，別に米国籍の職員が実際の破棄行為の立会人として署名することを要す。

964. 2　極秘及び秘資料の破棄

特に定めのない限り，極秘及び秘資料の破棄については文書カバーに破棄の記録を残す必要はなく，

保安局又は地域別保安担当官の記録表に記入するものとする。ＮＡＴＯ情報，原子力情報等特別な規則の定めに従う情報は，破棄処分の事実が定めにより記録される。

964.3　焼却用袋（burnbags）の使用

破棄すべき全ての秘扱資料は，ワープロのリボン容器や通常のタイプライター用リボン・カートリッヂを含め，焼却用袋に入れる。この袋は見分け易いものとし，焼却用に利用されるまでは関係資料と相応した保護手段により，保全すべきものである。

964.4　破棄処分の方法

秘扱資料は，通常，マイクロ・フィルムを例外として，焼却又は分解により破棄される。

秘扱マイクロ・フィルムの破棄処分は焼却又は化学処理，すなわち特定期間，承認された化学溶液中への浸漬で行われる。

964.5　秘扱磁気式保存装置の破壊

秘扱データの処理に用いられた磁気式データやプログラムの保存装置は，これを破壊するために別途制定された国務省ガイドラインにより処分するものとする。

965　在外公館の報告及び事故文書の報告

秘扱資料が紛失していたり，事故を発見した職員は誰でも，当該部局又は在外駐在の保安担当官に届け出るものとする。

機密又は暗号情報の事故の場合，緊急報告が必要となる。

保安担当官への報告には下記を記載のこと。

a．情報がいかなるものであるかの記述，可能であれば日付，件名，出所，宛先，汎例表示，秘扱区分，資料種別（電報，覚書，電信等）および開示の影響による損害査定。

b．紛失または不明の場合，紛失認知の日時と状況，最近の資料取扱いと資料にアクセスできる者，資料の所在を探る措置等を詳述のこと。

c．事故発生と考えられる場合，事故を生ずるに至った状況，情報にアクセスしたり，したかもしれないと思われる者，事故か否かを決定する手段，当該情報の重要性等を詳述のこと。

d．暗号情報の紛失又は事故の場合，通信局にも事故報告を行うこと。在外からは電報により報告のこと。

e．事故原因の可能性として自動化情報システムが関係していると思われる場合は，情報システム保安要員にも報告のこと。

966　公認されていない開示の報告

966.1　一般的手続

認められていない者に対し，国内部局や在外公館等が秘扱情報を開示したり，開示の疑いを持たれた場合，直ちに詳細報告を国務省では保安担当次官補，ＡＩＤでは保安局局長に行うこと。

966.2 非公認開示の報告書

非公認開示の報告書には以下を記載のこと。

a．判明していれば事件発生日

b．判明していれば文書ないし情報を提供又は開示した者（単，複数）及び当該情報はどのようなものかの記述

c．事故となった情報の主題と秘扱区分

d．非公認開示に関係している刊行物（新聞，技術雑誌，報告書等），スピーチ，説明報告等

e．当該開示が及ぼす影響

f．必要な場合，再発防止措置

g．必要に応じ追加の紙面を加える。

970 秘扱資料の物理的保護

971 秘扱資料の保管

971.1 一般要件

a．データ処理システム，ワード・プロセシング・システム，磁気処理システム等によるものも含め，秘扱情報は，許可されていない者が自由にそれにアクセスするのを防ぐ条件下でのみ利用，保持，処理，保管される。

b．秘扱資料は，在外においては，満足できる破壊能力を備えた応急処理設備がない限り，一昼夜通常の状態のままで保存してはならない。

c．秘扱資料は，公認された者自らの管理と監視下にないときは，承認された施錠格納容器中に保管すべきこと。地下貯蔵室にそのまま保管しておくことは，シュレッドしたり，外交パウチに入れて封緘しておく場合は別として，特に保安局や通信局の書面の許可がない場合は認められない。

d．秘扱資料には全て表紙（cover sheet）を付ける。

e．郵便受発信センター（post communications center）内にある通信整理ロッカー（message distribution locker）中に秘扱資料の確実は保管を行う責任は，そのロッカーが配属されている役所から出向している職員が負う。

971.2 機密文書

a．国内の場合

機密文書は，スリー・ウェイ・ダイアル式の組合せ錠付鉄製ファイル・キャビネットに保管するものとし，できればアラーム付立入規制区域に置くのが望ましい。

b．海外の場合

海外においては機密文書は，外交特権を認められた建物内で，認可された保管室内の，スリー・ウェイ・ダイアル式の組合せ錠付容器中に保管する。保管庫の位置要件に対する免除を受けるとき

は，地域別保安担当官の書面による承認が必要である。機密文書でＡＩＤ在外事務所宛伝達されるものはない。

971.3 極秘文書及び秘文書

a．国内の場合

機密文書用に公認された保管法によるか，公認された安全ファイルによるか，もし建物が保安上身元の明白な米国人公民である職員により24時間管理されているとすれば，保安用認可済組合せ南京錠付のカンヌキ式キャビネットの中に入れるかのいずれかによる。

b．海外の場合

機密文書用に公認された保管法によるか，キャビネットの位置が保安用に認可された場所にあるか，又は米国人公民である職員によって24時間その地区への立入が統制されている場所であれば，保安用認可済組合せ南京錠付のカンヌキ式キャビネットの中に入れるかのいずれかによる。

971.4 正規雇傭でない者による秘扱資料の保存

秘扱情報に関連する作業に携わるコンサルタントや請負業者は，保安局が承認を与えない限り，自分の事業所の構内で，秘扱資料を一昼夜にわたって保存してはならない。

また保安局の承認を得たときを除き，いかなる秘扱情報も，正式に定められた構内を離れた場所で，コンサルタントや請負業者の利用に供したり，これらの人宛に送達してはならない。

972 保安設備の組合せ錠の変更

a．格納容器とドアの組合せ錠の組合せ変更は，この組合せにアクセスできる当局により，下記いずれかの場合に実施できる。

(1) 施錠が最初から行われているとき。

(2) 組合せを知っている職員の雇傭が終了したり，もはやアクセスを必要としない任務に人事異動したとき。

(3) 許可されない者がその組合せを知ったか，知ったのではないかとの疑惑をもたれたとき。

(4) 少くとも12カ月に１回の頻度で変える。

(5) 装備一式が使用されなくなったとき。

b．組合せは別途定める保安カードに記録することとし，この組合せの記録は保管が認められている秘扱資料の最高部類同等のレベルで，秘扱いとするものとする。

保安カード及び，保管所内に貼り付けたカードを除き，組合せをそれ以外に記録することは禁じられている。組合せは全て記憶しておかねばならない。

c．略

d．組合せを知っている職員名は安全ファイル・キャビネット抽出し内部，保管室ドア内側，かんぬき式キャビネット上部抽出し内側に貼示される。

973　公的構内からの秘扱資料の持出し

973.1　一昼夜にわたる保管

a．秘扱資料は公用の会議，協議の実施上必要となる場合を除き，公的構内から持出してはならない。協議等終了後は直ちに安全な保管設備内に戻さねばならない。個人が一昼夜にわたり個人用に保管してはならない。

b．秘扱資料を公的構内から一昼夜にわたり持ち出すには，保安局又は地域別保安担当官の事前の承認を要す。

973.2　永久的離任時の証明

職員は，職制上の等級にかかわりなく，配置換え，辞任，退職等により職務を離れるとき，職務整理手順の一部として下記事実の証明をしなければならない。

a．秘扱資料が職場から持出されていないこと。

b．秘扱資料が個人用に使用されていないこと。

c．規則に違反して秘扱資料を送達していないこと。

974　秘扱情報の保全（ safeguarding ）

974.1　一般的手順

a．秘扱資料の使用，保管に責任を有す職員は，当該資料に事故のないよう万全の注意を払うこと。

b．秘扱資料は人がいない部屋に放置したり，充分な保護のない部屋に放置したり，保安上身元の確かな職員以外の者に占有された場所に放置してはならない。

974.2　注意事項

a．“開錠中”又は“閉錠中”の標識を秘扱資料の各収納庫に掲示する。

b．保安用チェック・シートを秘扱資料収納庫に取付け，開閉に責任のある担当者はシートに開閉を記入する。

ワード・プロセシング・システムで処理される秘扱情報も，一日の業務終了時に適切に保全されるべきこと。

c．秘扱資料の収納庫のある部屋が無人になる前に，収納庫は施錠されるべきこと。

閉錠は二重にチェック（ double check ）すべきこと。

d．保管設備又は錠設備の欠陥等は直ちに保安担当官に報告のこと。この補修には身元の確かな者のみを用いること。

e．保安用収納容器の使用をやめる場合は，秘扱資料全てがそこから取出されていることを徹底して確認すること。

974.3　就業時間後と昼食時間

a．秘扱資料は認可された保管収納容器以外の所，たとえば机の中等に置いてはならない。

b．秘扱資料作成に関連した処分可能の材料，例えば粗案草稿，速記原稿，カーボン紙，コピー，謄

写版原紙等は部屋が無人になる前に適切な保管用収納庫に入れて保管し，施錠する。タイプライター用リボンや録音用材料も同様である。

秘扱文書，一般扱文書の全てを確実に整理でき，効率の高い行政活動を図ることが可能になるという意味からも，このやり方は重要であり，“クリーン・デスク政策”を強力に推進している。

c．就業時間終了後，施錠を終えたドアの鍵は全て警備隊に引き渡し，正当と認められる者以外の者には鍵は貸出されない。

974.4　終業時保安点検

974.4－1　点検報告

a．終業時には警備員によるチェックの前に，保安点検を行う。

b．この基本的要件の履行のため，米国及び在外勤務地においては，監督官は週番制により部下を指名し，終業時の事務所保安点検を行わせる。被指名者は保安点検報告様式を使用し，点検結果を記録にし，点検終了と同時に保安担当官宛提出する。

974.4－2　違反の報告

違反の発見自体は保安に反するものではない。

974.4－3　職員の責任

a．終業時保安点検は最低限下記のことを行う。

(1)　秘扱資料収納庫の全ての点検を行う。

(2)　机の全てについて，机上及び全ての抽出しの内部を点検し，秘扱資料が除去されているのを確認する。

(3)　事務所の他の部分を肉眼で点検する。

b．秘扱資料の保管担当者は保管を確実にする責任を有するが，終業時保安点検者も保管者と共同責任を負うものとする。

974.4－4　要件適用の除外

特定地区に異常に多数の収納庫が存在したり，僅少の人数しか配置されていなかったり等の物理的，人員的問題等を根拠に本件要件の適用除外を求めるときは，書面により保安局又は地域別保安担当官に要請するものとする。

974.5　会　議

a．秘扱情報ないし資料がかかわる会議を実施する際は，下記事項を確実にするため万全の注意を払うべきこと。

(1)　技術的安全を図るため，公的な構内にて開催すること。

(2)　秘扱情報，資料の保護を図るため，適切な物理的保安措置が実行されること。

(3)　参加者は当該情報，資料にアクセスする資格があること。

b．当該会議を実施する部門から，下記の場合にはいつでも，保安担当官へ事前の通知（及び関係先への通知を含む）を行うこと。

(1) 秘扱資料が定常の保管場所から会議場へ移される場合。

(2) 参加者が外交官，領事等として派遣されている米国国籍公務員である場合を除き，当該会議を召集あるいは実施する担当官により，参加者の身元調査を実施済であるが，そのことを参加者自身が知らない場合。

975 物理的安全

975.1 カメラ

カメラは保安局又は地域別保安担当官の事前の承認を得ない限り，規制地域，規制建物又は秘扱資料のある部屋への持ち込みは許されない。

975.2 一括規制

異常又は緊急事態においては，保安局又は地域別保安担当官は，上級権限者の承認を得て，外部の物体が米国政府施設に導入されないよう，また秘扱資料が持出せないよう規制を課すことができる。

975.3 職員の身分証明

職員の身分証明書（ＩＤカード）は保安局又は地域別保安担当官により発行，管理される。

975.3－1 職員の建物への出入

職員は，建物又は規制地域に入る場合，求めに応じ，いつでも，警備員，受付，及び他の職員にＩＤカードを提示する。

975.3－2 就業時間外の建物への立入

a．時間外に建物から出る時，入る時はＩＤカードの提示の他，登録台帳に署名をする。

b．外国籍職員が正規の時間後も在外公館内で仕事をするよう求められた場合，及び臨時職員，請負業者等が就業時間外に建物に入ったり，残留を求められた場合は，その作業を命ずる担当官は地域別保安担当官，又は保安局，又は在外公館保安担当官の同意を得，かつ出入者はすべて登録台帳の出と入の所に各々署名しなければならない。

975.3－3 身分証明書の紛失

職員の身分証明書の紛失の際は，ワシントンであれ，在外であれ，保安局身分証明課宛直ちに報告しなければならない。報告では紛失状況，回収努力状況説明も付すものとする。

965.4 来訪者

就業時間後は，秘扱資料又は活動を内蔵する建物には，米国籍職員による護送がない限り，入場は許可されない。

通常，就業時間後の来訪者は警備員の机上で記帳を求められる。

976 事務所移転に係る保安計画

事務所移転の保安計画は，関係保安担当官により立てられ，承認される。

この計画では，秘扱資料の収納庫が確実に施錠されていること，移送中は米国籍職員が付き添うこ

と，資料の受け渡しも米国籍職員の手により行われることを要件とする。

980　通信の保安（COMSEC）

981　権　限

a．独立した省庁の長官は通信システムの保安措置を講ずる責任を有する。

b．電報の受発信に使用される暗号情報は法律により保護される。

982　責　任

982.1　通信保安部

通信保安部は通信保安管理のための規則，手続の制定に責任を有す。

982.2　通信保安（COMSEC）担当官

982.2－1　任命

暗号又はその他の通信保安関係資料を取扱う在外公館長及び主要高級職員は，COMSEC担当官を任命するか，自身でその任務に当るかする必要がある。COMSEC担当官は暗号解読権限が与えられる。

982.2－2　責　任

COMSEC担当官は，通信保安規則と手続とが，国内各部局，在外とを問わず，確実に守られていることを確認する責任がある。

982.2－3　違　反

通信規則又は手続上のいかなる違反も所定様式にてCOMSEC担当官から通信保安部宛報告しなければならない。かかる違反により，秘扱情報，行政統制された情報が危くなった場合，公電にて報告しなければならない。

982.3　通信保安（COMSEC）管理官（Custodian）

982.3－1　任　命

暗号又はその他の通信保安資料を保管する在外公館長及び主要高級職員は，COMSEC管理官を任命するか，自身でその任務に当る必要がある。暗号解読許可を与えることが，任命の前提条件となる。

982.3－2　責　任

COMSEC管理官はCOMSECのために発せられる全ての資料の保管・管理に責任を有す。

982.3－3　管理責任の移管

管理官の離任の少くとも30日前に，新管理官の任命が行われる。新旧両管理官は全資料を閲覧点検する。

983　秘扱電報と行政統制された電報の伝達

983.1　電　送

秘扱電報及び行政統制された電報は電送前に暗号化しなければならない。

983.2　外交パウチ又は郵便による伝達

a．秘扱電報及び行政統制された電報の通常の伝達は，同種の文書の伝達に関する規則に従って行うものとする。

b．暗号電報は外交パウチ又は郵便施設を利用して伝達してよい。伝書使が帯同するクーリエ便がないときは，この方法が早い。

984　秘扱電報及び行政統制された電報の保護

前掲の950，960，970の各項とも秘扱情報及び行政統制された情報の保全と配布の規則を定めており，電報についてもこれに準ずる。

985　暗号解読許可

a．暗号資料は高度の保護が与えられている。

b．暗号解読許可は暗号情報へのアクセスの正式な認可である。

c．長官級の幹部は業務上暗号解読許可を与えられている。

d．暗号解読許可を有する者は，“知る必要”のある事項のみにアクセスを有する。

985.1　暗号解読許可責任

電信課は正式な暗号解読許可を発給すると共に，暗号解読者に必要な通知を行う。

985.2　解読許可基準

暗号解読を許可される職員は，米国籍を有し，充分な背景調査を経た上で，機密情報にアクセスしうる者でなければならない。

985.3　解読許可のカテゴリー

解読許可のカテゴリーは下記2つに類別される。

985.3－1　暗号使用許可

暗号システムあるいは機器の操作，保守を行うことを認可したもの。

985.3－2　暗号アクセス許可

暗号解読，暗号へのアクセスを認可したものであるが，暗号使用許可を構成するものではない。

985.4　有効期間

985.4－1　“アクセス”許可

暗号のアクセス許可は，所定の職務に在る者の任期中のみ効力があるものとするが，理由があれば早期に取消すことができる。

985.4－2　“使用”許可

電信専門官及びその他の担当官共に，所定の職務在任期間中のみ有効とするが，理由があれば早期に取消すことができる。

985. 4 － 4　仮許可

緊急事態にあっては，“使用”，“アクセス”いずれの許可も，緊急事態期間中のみに限り，長官級高級職員により仮許可の形で与えることができる。

985. 5　暗号使用許可

使用を許可された職員は，使用対象の暗号システムにおいて充分な訓練を受け，習熟していなければならない。

985. 5 － 1 ～ 4

国務省は暗号任務従事職員の充分な訓練を行うと共に，在外又は国内の勤務先に対し，当該職員に“暗号使用許可”が発給されている旨の通知を行う。

985. 6　暗号へのアクセス許可

査察官，保安担当専門官，会計検査官等が任務に従い派遣される出張先には，“暗号アクセス許可”が発給されている旨の通知を行う。

986　通信保安資料管理

通信保安資料の効率的かつ安全な利用を図るため，その資料の作成，保管，取扱，伝達，処分，責任等が規制されている。

990　保安規則の管理

991　保安局

保安局は秘扱情報の保全のための施設，手続，統制等について，制定，検討，検査，助言の任務を負い，かつ国内，在外でのこれら規則の施行指導に責任を有する。

992　駐在地保安プログラム

在外の各駐在地では保安担当官を選任し，保安任務の実行に当たらせる。

993　国内保安プログラム

主要業務部門ごとに保安担当官を選任し，保安任務の実行に当たらせる。各担当官は，保安局との連絡に当ったり，担当部門の保安計画の全般的行政管理を行う。

994　職員への保安業務指導

994. 1　新規採用者

職員全員に対し，本件規則について相当程度の深度までブリーフィングを行うことが必要である。各新規採用者は，就任の際，保安業務請書を読み，署名をすることが求められる。

994.2　離任職員

退職する職員，連続60日以上職場を離れていた職員にも保安業務の再確認，すなわち，退任に当って秘扱資料全てを公的管理場所に返還すべきこと，秘扱情報について知っていることを退職後も引続き保全する責任の認識程度等の確認が行われる。

995　保安規則違反防止プログラム

995.1　略

995.2　保安検査

国内及び海外において，特に指定された者が保安規則が適切に守られていることを確認するため，就業時間内外に立入検査を実施することがある。

995.3　違反事実の報告

検査の結果，違反行為が発見された場合，保安当局へ違反通知報告書が送付される。この違反通知報告書は一般扱いである。

保安当局は審査後，違反記録書を当該部門の責任の所存を申し立てられた者に送付する。

この本人は違反容疑について不服を申し立てることができる。責任の最終判定が下されるまでは，違反記録書は違反関係ファイルに保管される。責任がないとの判定が出た場合は，保安局はその旨本人に通知し，関係記録を修正する。

995.4　他省庁からの出向職員による違反

他省庁からの出向職員による違反の場合も，上記と同じやり方で報告，処置される。

995.5　保安規則違反の判定

保安規則違反の判定は保安局が行う。

995.6　通信上の違反

暗号資料の紛失，盗難，許可なく目を通すこと，又は暗号化されないままの秘扱情報の通常通信手段による伝達等は極めて重大な違反であり，国務省電信課宛直ちに報告が必要である。

995.7　懲戒措置

a．違反の事実が認められた場合，人事規程の定めるところにより，下記のいずれかの措置が取られる。

(1)　戒告

(2)　けん責

(3)　給与支払停止

(4)　解雇

b．違反は発生日より起算して２年間は懲戒の対象となる。戒告は保安局から，過去２年内の違反行

為2件以下の者に発出される。

c．～d．略

995.8　行政統制された資料に関する違反

a．LOU（Limited Official Use）表示の付いた資料は秘扱資料ではなく，かかる資料の保管に若干の落度があっても，それをもって保安規則違反にはならない。

b．違反があった場合は秘扱資料に関する違反と同じ方法で処理される。

996　略

以　上

9. Voluntary Foreign Aid Programs 1985,

Report of American Voluntary Agencies Engaged in Overseas Relief and Development Registered with the Agency for International Development 抜すい

（USAIDから民間国際協力関係団体への支援・資金供与実績の公表例）

Report of American Voluntary Agencies
Engaged in Overseas Relief and Development
Registered with the Agency for
International Development

Voluntary Foreign Aid Programs

1985

Bureau for
Food for Peace
and Voluntary
Assistance

Agency for International Development
Washington, D.C. 20523

Agency for International Development
Washington, D.C. 20523

Voluntary Foreign Aid Programs

Report of American Voluntary Agencies Engaged in Overseas Relief and Development Registered with the Agency for International Development

M. Peter McPherson
Administrator
Agency for International Development

Julia Chang Bloch
Assistant Administrator
Bureau for Food for Peace and Voluntary Assistance

This Report Includes:

Register of Voluntary Agencies

Who they are and what they do

The rules governing the registration of nongovernmental, nonprofit agencies engaged in voluntary foreign aid are promulgated in Part 203, Chapter II, Title 22, Code of Federal Regulations. Such aid includes projects and services of development, relief, and rehabilitation to needy nationals and refugees in health, education, welfare, agriculture, industry, emigration, and resettlement. The register consists of the following agencies:

Accion International/AITEC
1385 Cambridge Street
Cambridge, Massachusetts 02138
(617) 492-4930

Accion International/AITEC supports the smallest scale economic activities of low-income people through credit, basic management training, and technical assistance programs in Latin America, the Caribbean and the United States. Now in its third decade of development, Accion assists street vendors, micro-business owners, subsistence farmers and other self-employed men and women in gaining access to the skills and resources needed to improve their own economic futures and those of their families.

Accion provides training and consultation to government institutions, private voluntary organizations, banks, community groups, and other private institutions seeking to work with micro-business people. Through a new development education program, the America Dialogue, Accion brings together private and public sector leaders from this hemisphere to discuss key development issues and to explore ways of promoting the economic initiatives of the poor.

Adventist Development and Relief Agency
6840 Eastern Avenue, N.W.
Washington, D.C. 20012
(202) 722-6770

Assists in rehabilitation for the needy through self-help projects. Operates and provides equipment and material aid for programs in education, agriculture, health care, community development and social welfare. Assistance is given to countries in Africa, Asia, Latin America and the Middle East.

African-American Institute
833 United Nations Plaza
New York, New York 10017
(212) 949-5666

Assists and promotes African manpower development through a variety of programs providing long- and short-term academic and technical education for Africans, both in the U.S. and in Africa. Brings African leaders to the U.S. for short-term visits, conferences, etc. Organizes exhibitions of African art. Conducts programs to improve the status of African women. Offers services to American and African traders, bankers, investors and other entrepreneurs. Organizes conferences bringing African and American leaders together to discuss issues of common concern. Provides special attention to informational needs of U.S. media and elected officials. The Institute is supported by contributions from individuals, corporations and philanthropic foundations; endowment income; and U.S. Government contracts for specific training and visitor programs.

African-American Labor Center
1125 15th Street, N.W., Suite 404
Washington, D.C. 20005
(202) 429-0050

The objectives of the Center are to support the development of free, democratic, self-sufficient, responsible and effective trade unions in Africa and to enable trade unions to participate in the process and benefits of economic, social and political development. General assistance in construction, housing and planning, cooperatives, credit unions and loans, education, industrial development and management, and material aid are extended by the Center to most African countries.

African Medical & Research Foundation
420 Lexington Avenue, Suite 556
New York, New York 10170
(212) 986-1835

AMREF provides assistance to governments, international agencies, and NGOs throughout East Africa in nearly 50 different health projects. These are conducted in Kenya, Tanzania, Uganda, Sudan, Ethiopia, Somalia, and Zambia. Programs include primary health care and training of community health workers; training of rural health staff through continuing education, teacher training, and correspondence courses; development, printing, and distribution of training manuals, medical journals, and health education materials; application of behavioral and social sciences to health improvement; airborne support for remote health facilities including surgical, medical, and public health services; ground mobile health services for nomadic pastoralists; medical radio communications; health project development, planning, and evaluation; consultancy services.

African Wildlife Leadership Foundation
1717 Massachusetts Avenue, N.W., Suite 602
Washington, D.C. 20036
(202) 265-8394

Provides funds and resources for the education and training of young Africans in managing and protecting their wildlife. Supports research, conservation education programs and two colleges of wildlife management.

Africare
1601 Connecticut Avenue, N.W., Suite 600
Washington, D.C. 20009
(202) 462-3614

Supports the development of water resources, increased food production, the delivery of basic health services and emergency assistance to refugees in rural Africa. Provides training and technical assistance, as well as start-up supplies and equipment. Has worked in some 22 African nations since establishment. Field offices in Burkina Faso, Chad, Mali, Niger, Rwanda, Senegal, Somalia, Zambia and Zimbabwe.

Summary of Support and Revenue

U.S. Voluntary Agencies Registered with the Agency for International Development

Agency	Grand Total	U.S. Government Support: A.I.D. Freight	P.L. 480 Freight	P.L. 480 Donated Food	U.S. Gov. Excess Property	U.S. Gov. Grants	U.S. Gov. Contracts	Other Governments & Int'l Org.	Donated Services	Donated Supplies & Equipment	Private Contributions	Private Revenue
Total All Agencies	2,467,529,406	7,643,874	133,876,743	367,514,300	22,799,425	244,532,863	86,783,565	138,443,400	22,538,349	174,196,842	990,953,035	278,247,010
ACCION International/AITEC	1,665,482					412,566	145,156	215,831	234,000		539,640	118,289
Adventist Development & Relief Agency	44,838,839	671,559	6,571,719	16,701,818	356,646	3,877,714			4,884,116	6,191,036	5,282,852	301,379
African-American Institute	14,403,563					3,058,848	9,058,929	65,605	884,350		810,015	525,816
African-American Labor Center	6,748,081						5,257,014	1,250,000			241,067	
African Medical and Relief Foundation	7,050,489					679,127	1,133,192	3,917,231		50,000	773,358	497,581
African Wildlife Leadership Foundation	1,203,235										980,401	222,834
AFRICARE Inc.	8,444,826	9,753				5,837,098		209,862	253,356	283,356	1,793,555	57,846
Aga Khan Foundation, USA	1,433,937										1,220,812	213,125
Agricultural Cooperative Development International	6,031,426					2,345,084	3,537,420				78,338	70,584
Aid to Artisans	171,311					159,961					7,633	3,717
America's Development Foundation	690,064					150,000			119,000	322,855	81,336	16,873
America-Mideast Educational & Training Services (AMIDEAST)	29,258,908					6,823,063	5,988,867	13,326,096			49,550	3,071,332
American Association for Bikur Cholim Hospital, Jerusalem	722,748										722,748	
American Committee for Shaare Zedek Hospital in Jerusalem	5,713,034	21,143				244,999					4,260,126	1,186,766
American Dentists for Foreign Service	541,796									434,078	40,588	67,130
American Friends of Kiryat Sanz Hospital	2,563,268							200,000		130,000	1,816,205	417,063
American Friends Service Committee	18,499,407	18,569						4,590		490,534	14,138,217	3,847,497
American Institute for Free Labor Development	14,280,265					1,424,584	11,476,498	1,078,516			300,667	
American Jewish Joint Distribution Committee	44,046,231		20,244	97,519			440,940			1,760,685	40,339,836	1,387,007
American Leprosy Missions	4,168,599										3,938,598	230,001
American Near East Refugee Aid	2,023,869					938,379				500,278	555,491	29,721
American ORT Federation	13,183,967	124				909,749	772,484				3,296,535	8,205,075

NOTE: These data represent the 12 month period of the fiscal year of the registered agencies and vary from agency to agency. The statistics contained in this statement are compiled from registered voluntary agency reports submitted as a requirement for continued registration. Data on income have been abstracted from the Statement of Support, Revenue and Expenditures (C-100), prepared by registered voluntary agencies which correspond to the individual agency's own fiscal year. "Donations of supplies and equipment" are those donations from private sources. Under "private contributions and other income" the other income may be derived from stocks, investments, direct bequests, interest on bank accounts, etc. The statistics on income from U.S. Government resources may vary from U.S. Government program statistics inasmuch as the voluntary agencies' fiscal reporting systems are not comparable to that of the U.S. Government.

*Recently registered: No report due.

Agency	Grand Total	U.S. Government Support: A.I.D. Freight	P.L. 480 Freight	P.L. 480 Donated Food	U.S. Gov. Excess Property	U.S. Gov. Grants	U.S. Gov. Contracts	Other Govern-ments & Int'l Org.	Donated Services	Donated Supplies & Equipment	Private Contributions	Private Revenue
American Red Magen David for Israel	5,429,084	276,078									4,400,503	752,503
American Schools of Oriental Research	687,341					50,000					329,101	308,240
Americares Foundation	20,928,616									20,246,849		681,767
Amigos de las Americas	1,106,054										1,106,054	
AMIT Women	3,940,000										3,355,000	585,000
Armenian General Benevolent Union	1,966,522					159,533					998,106	808,883
The Asia Foundation	23,866,091					14,056,547	1,681,790		56,466	6,695,905	862,497	512,886
Asian-American Free Labor Institute	5,303,448					5,213,567					77,500	12,381
Simon Bolivar Foundation	665,010					438,046			1,759		223,562	1,643
Boys' Clubs of America	13,511,077						87,118	5,796			10,189,119	3,229,044
Brother's Brother Foundation	14,563,573	10,800				24,000	119,531	2,000		14,244,492	154,171	8,579
Pearl S. Buck Foundation	4,107,687					234,105		175,427			3,511,750	186,405
Paul Carlson Medical Program	396,789									4,450	387,300	5,039
Catholic Relief Services	437,282,000	1,964,000	80,240,000	230,417,000		20,531,000		5,091,000		37,109,000	50,324,000	11,606,000
Centre for Applied Linguistics	3,695,997					188,698	3,246,841	32,014			2,987	225,457
Center for Development and Population Activities	1,238,568					478,663		102,924			265,470	391,511
Choi-Choi Foundation for Human Development	66,723										60,353	6,370
Christian Children's Fund	64,603,855										64,350,627	253,228
Church World Service	45,026,632	2,013,485	766,641	1,980,194		633,692	3,437,024	14,473		6,679,179	27,192,195	2,309,749
Community Development Foundation	72,272										72,196	76
Community Systems Foundation	274,068						230,692				23,044	20,332
Consortium for Community Self-Help	10,000										10,000	
Cooperative for American Relief Everywhere (CARE)	273,562,000	320,000	41,753,000	111,750,000		9,941,000		79,653,000		5,062,000	23,962,000	1,121,000
Cooperative Housing Foundation	3,328,774					286,382	641,616	2,340,095				60,681
Cooperative League Foundation	258,478										80,233	178,245
Cooperative League of the U.S.A.	4,519,314					3,545,048					974,266	
Coordination in Development (CODEL)	1,769,719					818,030			7,043		863,422	81,224
Council of International Programs for Youth Leaders Social Workers	680,267					409,696		120,255			150,316	
Credit Union National Association	17,476,343					2,840,096						14,636,247
Dental Health International	21,400									21,000	400	
Direct Relief International	6,984,082	36,044							252,937	6,006,077	576,337	112,687

Agency	Grand Total	U.S. Government Support: A.I.D. Freight	P.L. 480 Freight	P.L. 480 Donated Food	U.S. Gov. Excess Property	U.S. Gov. Grants	U.S. Gov. Contracts	Other Governments & Int'l Org.	Donated Services	Donated Supplies & Equipment	Private Contributions	Private Revenue
Domestic/Foreign Missionary Society for the Protestant Episcopal Church in the USA	45,383,000					4,098,000					34,281,000	7,004,000
Thomas A. Dooley Foundation/Intermed USA	878,267	55,055								191,420	603,763	28,029
Tom Dooley Heritage	194,791					43,180		14,931		54,514	74,561	7,605
El Congreso Nacional de Asuntos Colegiales (CONAC)	408,397					304,288	2,500		5,000		96,609	
Elwyn Institute*												
Esperanca, Inc.	1,168,634					223,326			306,785	48,305	556,487	33,731
Experiment in International Living	11,994,030					1,359,330	2,466,879	695,282			304,834	7,167,705
Eye Bank International	1,154,582										159,341	995,241
Eye Care, Inc.	430,300									123,674	306,626	
Feed the Children*												
Food for the Hungry	14,581,685		3,346,546	3,275,931						926,279	6,959,332	73,597
Food for the Poor*												
Foster Parents Plan	14,350,556					379,412		258,277			13,050,273	662,594
Foundation for the Peoples of the South Pacific	1,799,137					1,194,099				265,894	277,083	62,061
Friends of Children	672,843									514,667	144,913	13,263
Friends of Shanta Bhawan*												
Global Water	400,301										381,469	18,832
Goodwill Industries of America	3,988,236					83,260	826,355				239,280	2,839,341
Hadassah, The Women's Zionist Organization of America	53,967,725	154,744			15,868		1,498,482			336,191	44,277,661	7,684,779
Heifer Project International	6,122,554					802,834				433,406	4,362,584	523,730
HIAS	5,523,265						876,487	53,933			3,600,706	992,139
High Scope Educational Research Foundation	2,344,786					951,259					1,393,527	
Holt International Children's Services	5,195,040	6,891									1,040,739	4,147,410
Holy Land Christian Mission International	11,418,852					223,191			84,601		11,111,060	
Institute for International Development, Inc.	1,641,307					678,076		32,258	21,245		815,162	94,566
Institute of Cultural Affairs	2,413,910					18,065					2,118,338	277,507
Institute of International Education	92,619,238					21,164,386	6,250,622	6,719,056			2,158,554	56,326,620
International Agency for Apiculture Development	3,332										3,332	
International Aid	765,411									409,274	224,350	131,787
International Alliance for Children	206,657								60,050	857	52,530	93,220

Agency	Grand Total	U.S. Government Support: A.I.D. Freight	P.L. 480 Freight	P.L. 480 Donated Food	U.S. Gov. Excess Property	U.S. Gov. Grants	U.S. Gov. Contracts	Other Govern-ments & Int'l Org.	Donated Services	Donated Supplies & Equipment	Private Contributions	Private Revenue
International Child Care/USA*												
International Educational Development	31,000										31,000	
International Executive Service Corps	21,816,400					6,814,520			9,887,906		480,881	4,633,093
International Eye Foundation	1,678,696					891,772		158,175		137,674	459,336	31,739
International Federation for Family Life Promotion	634,626						601,449				33,177	
International Human Assistance Programs	4,466,430				50,846	2,606,230				1,335,225	436,198	37,931
International Institute of Rural Reconstruction	1,318,633					670,038		36,327	10,400		395,912	205,956
International Lifeline	162,154	2,490	12,240						36,569	59,658	51,197	
International Nursing Service Association	360,420					44,178		17,152		952	295,058	3,080
International Planned Parenthood Federation, Western Hemisphere	5,091,037					1,958,967		249,879			2,691,326	190,865
International Program for Human Resource Development	68,085										46,410	21,675
International Rescue Committee	16,490,702					7,328,000		1,542,000	120,779		6,750,685	749,238
International Social Service, American Branch	207,550										180,829	26,721
International Voluntary Services	1,676,190					722,927		32,789		204,212	716,262	
Katalysis Foundation*												
Helen Keller International	3,236,089					1,183,491					1,358,405	694,193
La Leche League International	2,551,943					110,209					94,519	2,347,215
Laubach Literacy International	2,660,540					12,246					557,020	2,091,274
Lutheran World Relief	21,394,033	599,315	959,247	2,804,655		1,280,097				6,870,588	8,572,050	308,081
MAP International	12,451,739	199,509								8,553,795	2,752,358	946,077
Meals for Millions/ Freedom from Hunger	2,474,950					650,000		133,696			1,610,613	80,641
Medical Care Development	3,121,608					835,469	387,056	889,958			329,901	679,224
Mennonite Central Committee	30,399,800	240,455						4,437,303		11,499,196	9,677,243	4,545,603
Mercy Corps International	2,927,417								18,540	2,389,910	515,375	3,592
Minnesota International Health Volunteers	104,028								11,259		90,632	2,137
The Moral Majority Foundation, Inc.*												
National Association of the Partners of the Alliance	4,246,613					3,119,025					976,159	151,429
National Council for International Health	959,071					654,845	6,750				51,379	246,097
National Council of Negro Women	468,886					321,533			125,800		20,048	1,505

Summary of Expenditures

U.S. Voluntary Agencies Registered with the Agency for International Development

Agency	Grand Total	Overseas Expenditures	Domestic Expenditures	Administration/ Management Costs	Publicity & Fund Raising
Total All Agencies	2,329,810,988	1,823,140,080	287,422,896	139,551,322	79,696,690
ACCION International/AITEC	1,691,760	1,406,038	87,117	141,179	57,426
Adventist Development and Relief Agency	44,292,675	39,788,961		2,745,878	1,757,836
African-American Institute	15,292,272	13,721,136		1,541,498	29,638
African-American Labor Center	6,723,478	5,633,291		1,090,187	
African Medical and Research Foundation	6,812,032	6,243,644		526,471	41,917
African Wildlife Leadership Foundation	1,042,446	784,739		168,196	89,511
AFRICARE, Inc.	5,056,252	4,086,273		893,919	76,060
Aga Kahn Foundation, USA	1,981,408	1,432,536	151,066	371,587	26,219
Agriculture Cooperative Development International	6,058,497	4,842,350	3,148	1,212,999	
Aid to Artisans	166,507	159,961		6,546	
America's Development Foundation	498,489	440,349		54,416	3,724
America-Mideast Educational & Training Services	29,004,512	27,475,410	58,323	1,470,779	
American Association for Bikur Cholim Hospital	743,969	578,373		37,360	128,236
American Committee for Shaare Zedek Hospital in Jerusalem	5,773,636	3,134,557		1,353,806	1,285,273
American Dentists in Foreign Service	243,411	233,859		9,552	
American Friends of Kiryat Sanz Hospital	2,936,940	2,428,204		143,673	365,063
American Friends Service Committee	16,505,928	4,644,263	7,748,271	2,432,654	1,680,740
American Institute for Free Labor Development	14,183,989	10,096,980	1,272,226	2,814,783	
American Jewish Joint Distribution Committee	44,108,570	41,019,053	100,100	2,989,417	
American Leprosy Missions	3,797,377	2,628,351		267,499	901,527
American Near East Refugee Aid	1,989,499	1,661,168	53,299	180,105	94,927
American ORT Federation	13,273,935	10,924,259	1,439,217	352,288	558,171
American Red Magen David for Israel	3,553,067	2,693,967	33,258	213,101	612,741
American Schools of Oriental Research	687,968	210,687	388,649	79,020	9,612
Americares Foundation, Inc.	20,752,895	20,664,522	14,596	11,856	61,921
Amigos de las Americas	1,054,623	805,839		171,171	77,613
Amit Women	3,741,000	2,189,000	937,000	413,000	202,000
Armenian General Benevolent Union	1,922,259		1,472,901	430,468	18,890
The Asia Foundation	23,099,838	22,100,652		963,947	35,239
Asian-American Free Labor Institute	5,293,957	3,617,686		1,676,271	
Simon Bolivar Foundation	620,767	544,548		76,219	

NOTE: These data represent the 12 month period of the fiscal year of the registered voluntary agencies and vary from agency to agency. Data has been abstracted from the Statement of Support, Revenue and Expenditures (C-100) prepared by registered Voluntary Agencies.

*Recently registered; no report due.

Agency	Grand Total	Overseas Expenditures	Domestic Expenditures	Administration/ Management Costs	Publicity & Fund Raising
Boys' Clubs of America	10,878,821	123,182	7,298,808	727,400	2,729,431
Brother's Brother Foundation	14,584,747	14,456,222		85,625	42,900
Pearl S. Buck Foundation	3,120,533	2,271,466	233,338	301,100	314,629
Paul Carlson Medical Program	436,771	374,590		51,885	10,296
Catholic Relief Services	407,384,000	398,132,000		8,136,000	1,116,000
Center for Applied Linguistics	3,603,228	1,664,207	1,173,812	765,209	
Center for Development and Population Activities	1,202,415	203,598	541,006	395,417	62,394
Chol-Chol Foundation for Human Resource Development	82,048	47,825		20,000	14,223
Christian Children's Fund	64,099,380	50,203,216	1,653,641	6,013,169	6,229,354
Church World Service	43,120,272	31,514,268	5,300,058	3,285,403	3,020,543
Community Development Foundation	72,272	72,272			
Community Systems Foundation	269,594	151,454	26,578	91,562	
Consortium for Community Self-Help	6,024	5,866		158	
Cooperative for American Relief Everywhere—CARE)	271,192,000	257,162,000		5,144,000	8,886,000
Cooperative Housing Foundation	3,473,958	1,855,432	348,292	1,270,234	
Cooperative League Fund	277,890	161,267	87,528	26,067	3,028
Cooperative League of the U.S.A.	4,772,385	2,832,529		1,939,856	
Coordination in Development (CODEL)	1,798,521	1,260,167	238,682	250,641	49,031
Council of International Programs for Youth Leaders and Social Workers	697,702		255,766	434,369	7,567
Credit Union National Association	19,319,942	3,458,184	8,318,097	6,652,127	891,534
Dental Health International	22,856	21,000	410	1,446	
Direct Relief International	7,268,967	6,976,332		191,261	101,374
Domestic/Foreign Missionary Foreign Society for the Protestant Episcopal Church in the U.S.A.	42,279,000	13,743,000	21,504,000	5,430,000	1,602,000
Thomas A. Dooley Foundation/Intermed-USA	955,382	637,628		169,155	148,599
Tom Dooley Heritage	278,736	263,665		7,257	7,814
El Congreso Nacional de Asuntos Colegiales (CONAC)	334,874	5,000	131,126	198,748	
Elwyn Institute*					
Esperanca	1,114,882	929,985		96,776	88,121
Experiment in International Living	11,610,786	7,807,252	909,244	2,084,197	810,093
Eye Bank International	1,229,139	24,076	1,073,021	103,758	28,284
Eye Care, Inc.	822,613	626,726		39,559	156,328
Feed the Children*					
Food for the Hungry	13,949,567	10,711,677	1,256,716	1,135,627	845,547
Food for the Poor*					

Agency	Grand Total	Overseas Expenditures	Domestic Expenditures	Administration/ Management Costs	Publicity & Fund Raising
Foster Parents Plan	14,207,576	10,218,772		1,461,575	2,527,229
Foundation for the Peoples of the South Pacific	1,802,729	1,588,283		204,149	10,297
Friends of Children	686,226	658,013	15,797	7,198	5,218
Friends of Shanta Bhawan*					
Global Water	376,281	300,000		72,718	3,563
Goodwill Industries of America	3,802,304	271,658	2,794,023	726,817	9,806
Hadassah the Woman's Zionist Organization of America	41,407,269	30,897,282	3,481,008	4,308,302	2,720,677
Heifer Project International	5,365,432	3,519,875	666,203	334,412	844,942
HIAS	4,229,752	1,765,301	1,740,963	420,361	303,127
High Scope Educational Research Foundation	2,526,805	479,663	1,375,321	671,821	
Holt International Children's Services	4,875,352	2,504,737	1,806,099	309,504	252,012
Holy Land Christian Mission International	11,549,719	6,961,026	1,025,339	675,669	2,887,685
Institute for International Development, Inc.	1,810,300	1,305,129	315,394	131,466	58,311
Institute of Cultural Affairs	2,547,734	383,202	1,929,266	135,522	99,744
Institute of International Education	91,719,443	49,686,299	39,716,795	1,756,753	559,596
International Agency for Apiculture Development	3,515	1,188		2,327	
International Aid	298,411	167,545	5,718	108,906	16,242
International Alliance for Children	212,569	62,794	97,959	51,816	
International Child Care/USA*					
International Educational Development	31,000	8,000	20,000	3,000	
International Executive Service Corps	21,549,807	19,131,166		2,314,150	104,491
International Eye Foundation	2,736,271	2,632,552		42,373	61,346
International Federation for Family Life Promotion	653,905	422,503	38,528	187,425	5,449
International Human Assistance Programs	4,673,871	4,259,458		328,473	85,940
International Institute of Rural Reconstruction	1,455,864	1,030,747		311,552	113,565
International Lifeline	127,113	112,872		13,824	417
International Nursing Services Association	369,412	65,071	224,178	31,359	48,804
International Planned Parenthood Federation/Western Hemisphere	5,004,681	3,767,097		1,161,110	76,474
International Program for Human Resource Development	86,671	25,438	45,000	16,233	
International Rescue Committee	16,060,614	7,311,402	7,335,867	794,113	619,232
International Social Service, American Branch	160,363		132,010	25,754	2,599
International Voluntary Services	1,676,783	1,472,107		187,429	17,247
Katalysis Foundation*					
Helen Keller International	2,629,490	1,889,380	254,728	264,441	220,941
La Leche League International	2,280,866	10,314	1,419,481	368,475	482,596
Laubach Literacy International	2,235,842	130,915	1,705,111	266,113	133,703

Agency	Grand Total	Overseas Expenditures	Domestic Expenditures	Administration/ Management Costs	Publicity & Fund Raising
Lutheran World Relief	18,449,887	17,434,230		827,601	188,056
MAP International	14,441,610	13,513,380		282,722	645,508
Meals for Millions/Freedom from Hunger	2,242,861	1,160,139	573,668	201,152	307,902
Medical Care Development	2,424,502	530,424	1,366,863	527,215	
Mennonite Central Committee	30,020,499	25,994,197	1,645,770	1,770,331	610,201
Mercy Corps International	2,958,976	2,686,226	142,459	81,354	48,937
Minnesota International Health Volunteers	104,564	93,858		9,729	977
The Moral Majority Foundation, Inc.[a]					
National Association of the Partners of the Alliance	4,090,036	3,343,549		658,129	88,358
National Council for International Health	979,097	108,619	617,934	250,666	1,878
National Council of Negro Women	467,381	467,381			
National 4-H Council	11,268,137	707,093	9,052,456	855,154	653,434
National Office for Social Responsibility in the Private Sector	827,915	270,949	390,379	166,587	
National Rural Electric Cooperative Association	30,402,935	3,685,621	23,649,641	3,067,673	
National Wildlife Foundation	39,044,000		34,549,000	1,606,000	2,889,000
Nature Conservancy	27,397,000	1,646,000	18,638,000	2,151,000	4,962,000
Near East Foundation	1,050,753	772,255		211,525	66,973
New TransCentury Foundation	4,548,973	3,552,193	487,902	508,878	
OBOR	91,199	62,738		20,563	7,898
Operation Bootstrap-Africa	267,480	168,418		35,135	63,927
Opportunities Industrialization Centers International	3,059,008	2,367,436	72,501	576,698	42,373
Overseas Education Fund	1,889,595	1,085,839	143,991	575,974	83,791
Pacific Ministries Development[a]					
Pan American Development Foundation	5,722,043	5,307,743		304,178	110,122
Partnership for Productivity	2,620,087	2,151,330	14,141	454,616	
Pathfinder Fund	6,541,289	4,857,470		1,587,438	96,381
People-to-People Health Foundation, Project HOPE	18,956,202	15,342,901	1,646,514	741,550	1,225,237
The Trustees of the Phelps-Stokes Fund	4,827,052		3,883,562	819,598	123,892
Pioneer Women	2,879,746	2,777,706	65,783	35,036	1,221
Planned Parenthood Federation of America	30,291,799	18,349,667	5,663,875	3,961,516	2,316,741
Planned Parenthood of New York City	9,176,491	282,000	7,784,263	529,460	580,768
Planning Assistance, Incorporated	196,271	142,780	3,022	50,469	
Population Council	18,487,317	6,586,466	6,345,572	5,431,983	123,296
Private Agencies Collaborating Together (PACT)	4,266,029	3,950,794		280,334	34,901
Program for Appropriate Technology in Health[a]					

Summary of Grants for PVOs

During 1982-83, the types of A.I.D. grant relationships available to U.S. PVOs from FVA/PVC and other A.I.D. bureaus, offices and Missions are described in the following. Registration with A.I.D. is a prerequisite for application for each.

Field Support for PVOs

With funding provided both through U.S.A.I.D. Missions and A.I.D./W regional bureaus, A.I.D. deals primarily with private and voluntary organizations at the country level through field support grants, a term which encompasses both operational program grants (OPGs) and co-financing program grants. In addition, there are two other modes which are occasionally used — contracts and cooperative agreements. The funding instrument chosen is determined by the intended relationship based on A.I.D.'s program objectives, not on the nature of the recipient (i.e. PVO).

Matching Grants

Matching grants are awarded to PVOs for a clearly conceived, evaluable, field-oriented program to be carried out in a number of countries, which is consistent with A.I.D.'s legislative mandate and supports a clearly defined, delineated program. Such a program may be as broad as the overall scope of the PVO's work or as specific as community-based health services or small enterprise development. The matching grant will normally allow a PVO to expand its program to new places and initiate new projects. Grants are awarded to PVOs with well-established development programs and with demonstrated private fund-raising ability. The grant may have a term of up to three years and is matching in the sense that A.I.D. will pay no more than 50% of the cost of the program. Through the Matching Grant, A.I.D. supports small enterprise development, local institution-building, and technology adaptation and transfer, directly and as they result from programs in agriculture and rural development, health, education and energy. Guidelines and selection criteria for this grant category are currently undergoing minor modification to reflect the Agency's nine years of experience with the program and the reality of federal budget reductions.

Partnership Grant

Partnership grants are essentially a refinement and an extension of the Matching Grant concept. To qualify, the PVO must have a successful record of implementing multiple, on-going relationships with the Agency. These grants are authorized for a five-year period, and are expected to enhance the PVO's role in addressing development priorities shared by A.I.D. Partnership grants are also matched in the sense that A.I.D. pays up to 50% of the cost of the activity.

Child Survival Grant

Beginning in FY 1985, competitive grants will be awarded to PVOs engaged in health programming as part of their international development efforts. Project activities are designed to demonstrably enhance the health status of children living in target areas through the delivery of a select number of simple, cost-effective technologies. Oral rehydration therapy and immunizations are the primary interventions delivered through the Child Survival grants. At least 25% of the project costs must be borne by the grantee.

Development Education Program

A competitive, matching small grants program, initiated in FY 1982, to increase the awareness of the American public of the social, political, technical and economic factors pertaining to world hunger and related development issues by supporting private and voluntary organizations in their efforts. The Development Education Program is targeted to program initiatives which facilitate broad public participation and imaginative educational approaches and to create outreach efforts directed to the media, educational associations and other important influence groups.

Other A.I.D. Relationships

Private and voluntary organizations carry out particular technical programs in fields of interest to A.I.D., such as family planning, health, energy and the like. For example, through the Office of Foreign Disaster Assistance, grants are provided to PVOs in support of disaster relief and rehabilitation activities. PVOs are also among the grantees under the American Schools and Hospitals Abroad Program. Consortia have proven to be effective vehicles for assistance to local projects in LDCs and A.I.D. supports PVO consortia in their efforts to promote coordinated planning for overseas development programs through the design, implementation and evaluation of small projects undertaken by member agencies on a cost-sharing basis. A.I.D. supports cooperative development organizations to enable them to play an important role in the development of LDC cooperatives by organizing local cooperatives and credit unions, strengthening cooperative federations, training cooperative managers and technicians, and encouraging the use of cooperative structures in development projects. These suppoort grants also strengthen the ability of U.S. cooperatives to attract and channel additional bilateral, multilateral and cooperative development funding. The Ocean Freight Reimbursement program reimburses PVOs for shipment of purchased or donated commodities used in their relief and development programs overseas.

Percentage of Funds Received from Non-U.S. Government Sources in Support of International Programs

The International Security and Development Cooperation Act of 1981 amended Section 123(g) of the Foreign Assistance Act of 1961 to establish a minimum non-U.S. Government (U.S.G.) funding requirement for the programs of U.S. Private and Voluntary Organizations (PVOs) funded from certain specified appropriation accounts. Stated simply, beginning January 1, 1985, PVOs must obtain at least 20 percent of their total funding for their international program from non-U.S.G. sources in order to qualify for grants set aside for PVOs (e.g., matching, operational program and co-financing grants). These grants are used to support PVOs as independent entities in their own right. A.I.D. also deals with PVOs as intermediaries in conducting A.I.D.'s program. These forms of support, such as institutional support grants to the labor institutes, family planning agencies and cooperative development organizations, are excluded from the 20% non-U.S.G. funding requirements.

A calculation of each registered PVO's status vis-a-vis this 20% requirement will be made annually based on documentation submitted as part of the annual recertification process for registration with A.I.D. Listed below are the percentage calculations for each PVO, computed on the basis of the 1984 audited financial documentation submitted to A.I.D. For purposes of determining PVO grant eligibility, A.I.D. maintains a separate listing which is updated as new financial information is submitted by the PVOs. Next year, percentages shown in this section will be based on the new private resource test as enacted in the FY 1986 Foreign Assistance Appropriations Act.

*Recently registered, no report due.

	%
Accion International/AITEC	62
Adventist Development & Relief Agency	58
African-American Institute	26
African-American Labor Center	100
African Medical & Research Foundation	88
African Wildlife Leadership Foundation	100
AFRICARE	22
Aga Khan Foundation, USA	100
Agricultural Cooperative Development International	6
Aid to Artisans	39
America's Development Foundation	100
America-Mideast Educational & Training Service (AMIDEAST)	70
American Association for Bikur Cholim Hospital, Jerusalem	100
American Committee for Shaare Zedek Hospital in Jerusalem	100
American Dentists for Foreign Service	100
American Friends of Kiryat Sanz Hospital	100
American Friends Service Committee	99
American Institute for Free Labor Development	45
American Jewish Joint Distribution Committee	100
American Leprosy Missions	100
American Near East Refugee Aid	100
American ORT Federation	100
American Red Magen David for Israel	100
American Schools of Oriental Research	79
Americares Foundation	100
Amigos de las Americas	100
AMIT Women	100
Armenian General Benevolent Union	0
The Asia Foundation	52
Asian-American Free Labor Institute	1
Simon Bolivar Foundation	28
Boys' Clubs of America	100
Brother's Brother Foundation	100
Pearl S. Buck Foundation	87
Paul Carlson Medical Program	100
Catholic Relief Services	70
Center for Applied Linguistics	0
Centre for Development & Population Activities	31
Chol-Chol Foundation for Human Development	100
Christian Children's Fund	100
Church World Service	98
Community Development Foundation	100
Community Systems Foundation	100
Consortium for Community Self Help	100
Cooperative for American Relief Everywhere (CARE)	54
Cooperative Housing Foundation	88
Cooperative League Foundation	100
Cooperative League of the U.S.A.	26
Coordination in Development (CODEL)	53
Council of International Programs for Youth Leaders & Social Workers	39
Credit Union National Association	100
Dental Health International	100
Direct Relief International	96
Domestic/Foreign Missionary Society for the Protestant Episcopal Church in the U.S.A.	78
Thomas A. Dooley Foundation/Intermed-USA	89
Tom Dooley Heritage	81
El Congresso Nacional de Asuntos Colegiales (CONAC)	100
Elwyn Institute*	
Esperanca, Inc.	66
Experiment in International Living	85
Eye Bank International	100
Eye Care, Inc.	100
Feed the Children*	
Food for the Hungry	60
Food for the Poor*	
Foster Parents Plan	97
Foundation for the Peoples of the South Pacific	30
Friends of Children	100
Friends of Shanta Bhawan*	
Global Water	100
Goodwill Industries of America	6
Hadassah—The Women's Zionist Organization of America	100
Heifer Project International	73
HIAS	100
High Scope Educational Research Foundation	2
Holt International Children's Services	100
Holy Land Christian Mission International	98

10. Current Technical Service Contracts and Grants

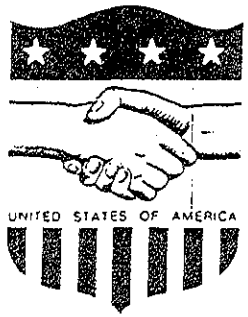
Active During the Period October 1, 1985 Through September 30, 1986 抜すい

（USAIDのコンサルタント契約等実績公表例）

Current Technical Service Contracts and Grants

Active During the Period October 1, 1985 Through September 30, 1986

Fiscal Year 1986



Office of Procurement

Procurement Support Division

U.S. International Development Cooperation Agency

Agency for International Development

Washington, D.C. 20523

W-443

TABLE OF CONTENTS

REPORT NUMBER: E340W43A

STATISTICAL SUMMARY

CURRENT TECHNICAL SERVICE CONTRACTS AND GRANTS

FROM: OCTOBER 1, 1985 THRU: SEPTEMBER 30, 1986

	NUMBER OF COUNTRIES	NUMBER OF CONTRACTS	AMOUNT IN DOLLARS *
WORLDWIDE	--	687	$1,501,720,558
ASIA	20	743	$372,363,162
NEAR EAST	15	373	$408,514,075
LATIN AMERICA	30	1458	$402,201,360
EUROPE	5	20	$25,826,461
AFRICA	47	838	$673,775,024
UNITED STATES	--	757	$121,990,778
TOTAL	117	4876	$3,506,391,438

1. TECHNICAL SERVICE CONTRACTS ARE AGREEMENTS ENTERED INTO BY A.I.D. WITH UNIVERSITIES AND TECHNICALLY QUALIFIED FIRMS, ASSOCIATIONS AND INDIVIDUALS FOR THE PURPOSE OF EMPLOYING THEIR SERVICES WHERE APPROPRIATE.

2. THIS LISTING DOES NOT INCLUDE CONTRACTS MADE BY BORROWERS UNDER DEVELOPMENT LOAN AGREEMENTS.

3. CONTRACTS FOR PERSONAL SERVICES OF INTERPRETERS ARE NOT INCLUDED BY NAME, BUT ARE COUNTED IN THE TOTAL NUMBER OF CONTRACTS SHOWN IN THE STATISTICAL SUMMARY.

4. ANY INQUIRIES OR CORRECTIONS SHOULD BE DIRECTED TO THE OFFICE OF PROCUREMENT, PROCUREMENT SUPPORT DIVISION, SUPPORT SERVICES BRANCH, WASHINGTON, D.C. 20523

* FUNDS ARE EXPRESSED TO THE NEAREST DOLLAR.

"Any USAID contractual documents and/or data sheets which were not received in SER/OP/PS/SUP by November 1, 1986 or which were received but were incorrect are not reflected in this publication."

ALPHABETICAL LISTING OF CONTRACTS AND GRANTS
WITH UNIVERSITIES, FIRMS, AND
NON-PROFIT INSTITUTIONS

CONTRACT NUMBER	CONTRACTOR NAME	TERM OF CONTRACT	AMOUNT IN DOLLARS	CONTRACT DESCRIPTION
LAC-0109-0-00-6047-00	A KLETT VISUAL AID	86/05/29-86/07/31	$9,064	VENDOR WILL PROVIDE PHOTO EQUIPMENT TO USAID/RWANDA
OTR-0000-0-00-6106-00	ABRAHAMS, KWYN	86/07/10-86/09/11	$9,918	CONTRACTOR SHALL PROVIDE PROCUREMENT POLICY ASSISTANCE IN REVISING AN AID HANDBOOK
OTR-0000-0-00-6133-00	ABRAHAMS, KWYN	86/08/28-86/10/27	$4,437	CONTRACTOR WILL REVIEW REGULATIONS GOVERNING COMMODITY PROCUREMENT
PDC-0000-I-11-3080-00	ABT ASSOCIATES, INC.	85/06/27-86/03/15	$85,910	CONTRACTOR SHALL ORGANIZE WORKSHOPS RELATING TO MONITORING AND EVALUATION OF WOMEN IN DEVELOPMENT (WID) EXPERIENCES
PDC-0000-I-15-3080-00	ABT ASSOCIATES, INC.	86/03/17-86/08/30	$37,200	CONTRACTOR SHALL ASSIST WITH DISSEMINATION ACTIVITIES OF THE STUDY OF AID'S EXPERIENCE IN WOMEN IN DEVELOPMENT
OTR-0089-G-SS-4340-00	ACADEMY FOR EDUCATIONAL DEVELOPMENT, INC.	84/08/28-86/01/28	$199,980	PROVIDE SUPPORT FOR U.S. TELECOMMUNICATIONS TRAINING SCHOLARSHIPS
OTR-0089-G-SS-5119-00	ACADEMY FOR EDUCATIONAL DEVELOPMENT, INC.	85/07/09-87/07/31	$800,000	PROVIDE SUPPORT FOR U.S. TELECOMMUNICATION TRAINING INSTITUTE SCHOLARSHIPS
AID/DSPE-C-0051	ACADEMY FOR EDUCATIONAL DEVELOPMENT, INC.	79/09/28-86/09/30	$4,160,662	TO PROVIDE ACCESS TO EFFECTIVE PRIMARY SCHOOL EDUCATION THROUGH USE OF MODERN COMMUNICATIONS MEDIA
OTR-0232-C-00-5163-00	ACADEMY FOR EDUCATIONAL DEVELOPMENT, INC.	85/09/25-90/09/30	$1,676,440	PROVIDE A SERVICE CAPABILITY RESPONSIBLE FOR PROVIDING INFORMATION SERVICES TO USAID MISSIONS AND STAFF
PDC-1406-I-28-4052-00	ACADEMY FOR EDUCATIONAL DEVELOPMENT, INC.	86/05/13-86/07/15	$19,998	TO ASSIST IN ORGANIZING A TWO-DAY BRIEFING ON DECENTRALIZATION OF EDUCATION SERVICES FOR AID'S LATIN AMERICA BUREAU
PDC-0230-G-SS-5099-00	ACCION INTERNATIONAL/AITEC	85/09/20-87/08/31	$156,247	SUPPORT A DEVELOPMENT EDUCATION PROGRAM WITH THE CORPORATE COMMUNITY IN SIX U.S. CITIES
DHR-1096-0-00-6025-00	ACE FEDERAL REPORTERS	86/06/10-86/06/12	$428	PROVIDE STENOGRAPHER SERVICES FOR BIDDERS CONFERENCE FOR DEVELOPMENT STRATEGIES FOR FRAGILE LANDS PROJECT
518-0062-C-00-6018-00	ACE SCIENTIFIC SUPPLY COMPANY	85/12/16-86/02/15	$16,500	CONTRACTOR PROVIDE MEDICAL SUPPLIES
OTR-0000-C-00-6127-00	ACROW CORPORATION OF AMERICA	86/08/13-86/08/18	$85,222	CONTRACTOR SHALL PROVIDE REPLACEMENT PARTS TO REPAIR THE TORBECK RIVER BRIDGE IN HAITI
391-0468-C-00-5040-00	AEGIS INTERNATIONAL DEVELOPMENT CORPORATION	85/08/05-85/12/05	$247,991	CONTRACTOR SHALL FURNISH AND DELIVER 17 JEEPS MANUFACTURED BY AMERICAN MOTOR CORPORATION TO KARACHI, PAKISTAN
515-0001-C-00-5609-00	AGRICULTURAL COOPERATIVE DEVELOPMENT INTERNATIONAL (ACDI)	85/09/10-85/11/22	$85,515	TO CARRY OUT A 58 DAY TRAINING PROGRAM IN THE U.S. FOR 20 COOPERATIVE STORE MANAGERS FROM COSTA RICA