First Draft
5 April 1950

[redacted]

CENTRAL INTELLIGENCE AGENCY
SECURITY REGULATIONS

Date 5 April 1950

I. GENERAL

1. CONCEPT OF SECURITY

A. Security, as applied to an intelligence organization, is defined as a condition which assures the safeguarding of valuable information and the protection of physical and human assets, the compromise of which might seriously impair the interest of the Nation. In the intelligence field, it is imperative that a true state of security exist in time of peace, as well as in time of war.

B. Even a partial compromise of security represents a loss which never can be regained--the damage is done. To prevent such a contingency requires the complete and unfailing cooperation of each and every member of the Central Intelligence Agency, irrespective of position. Any employee, through carelessness, negligence, or by relaxing his security vigilance, even temporarily, may cause vital information to fall into the hands of unfriendly interests who are always on the alert to take advantage of lapses. Aside from the potentially grave consequences which acts of this type may cause, much valuable documentary material assembled at the expense of great effort on the part of many members of this organization may be nullified completely. Therefore, it is the responsibility of each individual member of the CIA to train himself in the perpetual and unrelenting observance of all elements of security. Effective security is largely a matter of habit, the habit of discretion and care which has become second nature through constant usage. It must be cultivated by all employees if our mission and objectives are to be realized fully.

2. POLICY GOVERNING USE OF OFFICIAL DATA

A. All information received or compiled by the Central Intelligence Agency is official data and is the property of the United States Government. No officer or employee has any property interest in such information. The restrictions and prohibitions provided in this instruction apply not only to all intelligence information and material, but also to any statistical, administrative or general information, regardless of the fact that such information may already be a matter of general public knowledge. This shall also apply to all official data used or compiled by CIA and obtained from outside sources, public or private.

[redacted]

B. Official data are restricted to use in the performance of the official business of CIA and shall not be copied or removed from the files or from the premises of CIA except for official purposes.

C. No person connected with CIA shall accumulate in any official capacity, copies of documents containing any such data for inclusion in a personal file, nor shall any person appropriate to his personal use, any official data acquired by virtue of his connection with CIA.

D. Exceptions to the regulations contained in this instruction will not be made except upon written approval of the Director of Central Intelligence. Authority to release official data shall be limited to officials designated by the Director of Central Intelligence.

3. POLICY GOVERNING UNOFFICIAL PUBLICATIONS AND RELATED MATTERS. The following policies are announced for the guidance and protection of CIA personnel in the interpretation of the various paragraphs of the Secrecy Agreement, upon the provisions of which, at their own willing acceptance, employment is conditioned. These policies are necessary in order to establish a procedure for clearance of public statements, releases to the press, official or unofficial publications, speeches or similar undertakings which might result in inadvertent disclosure of classified information. These policies are further necessary to preserve the confidential nature of employee's official positions and duties and to prevent inferences of official policy on the part of CIA in connection with national or international problems. The involvement of CIA employees in controversial matters of widespread importance may not only reveal official position and duties but may be construed as indicating CIA official policy.

A. Publications and Utterances Relating to Intelligence

Except by special direction or authorization in the name of the Director, no person employed by, or assigned to the Central Intelligence Agency shall make a speech publicly, read a paper, or write for publication, the subject matter of which relates to intelligence or to the organization and functions of the CIA or other intelligence agencies.

B. Other Publications, Activities and Utterances.

Clearances must be obtained by written application with respect to addresses and publications believed to lie outside the prohibition set forth in subparagraph A. above. Such applications shall enclose, in appropriate cases, the actual text of the proposed address or publication. Clearances will also be obtained with respect to completing questionnaires and membership applications where information regarding present employment is sought; teaching or studying unofficial courses; attending conventions; engaging in private foreign travel for personal reasons; serving jury duty; and privately sponsoring

the entry of aliens into the United States. Applications shall be addressed to the Chief, Inspection and Security Staff, through the appropriate Assistant Director or Staff Chief, except as provided for in subparagraph C. below. Burden of proof that classified information will not be divulged rests with the applicant. Further, the applicant must establish that material to be publicized and the circumstances thereof do not involve controversial matters of national importance which might tend to disclose the author's official position and duties or appear to indicate by inference an official policy of CIA. This paragraph does not apply to extemporaneous addresses arising from requests which would be embarrassing to refuse, so long as CIA personnel so called upon discuss subjects which are in no way allied to activities of the CIA, and so long as neither the speakers' connection with CIA nor the subject of intelligence, nor national policy matters are mentioned.

C. Processing of Requests, Taking or Giving Unofficial Courses

Requests for approval of applications for the taking or giving of unofficial courses of study will be processed as follows:

1. To the Chief, Inspection and Security Staff, when the application covers courses having a bearing on intelligence activities, e.g., international politics, economics, languages, etc., or courses to be taken or given in the smaller tutoring type school.

2. To Assistant Directors and Staff Chiefs concerned when the application covers courses other than those indicated in paragraph 1. above when in their opinion no security implications are involved. The application and a copy of the letter of approval in these cases will be forwarded to the Inspection and Security Staff.

D. Announcement of Connection with CIA

In the event that clearance is granted under subparagraphs A. and B. above, CIA personnel will not, under these circumstances, allow themselves to be presented, indicated or introduced as connected with CIA except by special authorization in the name of the Director.

4. PENALTIES FOR NONCOMPLIANCE. In accordance with paragraph 5 of the Secrecy Agreement, and inasmuch as employment by CIA is conditioned upon compliance with it and with these Security Regulations, any failure to observe these regulations, or a disregard thereof, will subject the employee or employees involved to immediate dismissal or to such disciplinary action as may be imposed by the Director of Central Intelligence.

[redacted]

A. ADMINISTRATIVE ACTION. In cases of noncompliance with CIA security requirements, the Director of Central Intelligence may take administrative action as follows: (1) separation, (2) suspension, (3) reprimand or (4) such other administrative action as shall be deemed advisable.

B. LEGAL ACTION. In cases of violation of the provisions of the Espionage Act, persons attached to the Central Intelligence Agency are subject to criminal prosecution which may result in imprisonment, or a fine, or both, at the discretion of the court.

II. PROCESSING OF EMPLOYEES FOR ENTRANCE ON DUTY, LEAVES OF ABSENCE AND SEPARATIONS

5. SECRECY AGREEMENT

All personnel assigned to, or attached for duty with, the Central Intelligence Agency, prior to beginning their official duties will be required to execute a Secrecy Agreement which will be administered by the Director of Central Intelligence or his authorized representative.

6. SECURITY PROCESSING

A. PRELIMINARY INDOCTRINATION. Subsequent to the receipt of security approval, and upon completion of all other necessary administrative processing, the Personnel Office will notify an applicant to report for duty. Prior to the time the employee actually commences his duties with the office to which he will be assigned, the Personnel Office will instruct the employee to report to the Physical Security Branch, Chief of Inspection and Security Staff, for Security Processing. Upon arrival at the Physical Security, the individual will receive preliminary security indoctrination and processing as follows:

1. The employee will read the pertinent extracts of the Espionage Act of 1917, as amended and the CIA Security Regulations Manual. The Secrecy Agreement will then be read and executed under oath by the employee.

2. He will be fingerprinted.

3. He will be photographed.

Upon completion of the foregoing, the employee will be given an appointment slip instructing him to attend a security indoctrination class, which will be held within ten (10) days of his entrance-on-duty date. The employee will be requested to study carefully, and thoroughly familiarize himself with the instructions contained in the CIA Security Regulations Manual prior to attending the class.

[redacted]

B. INDOCTRINATION CLASS. The Security Indoctrination class is conducted under the auspices of the Chief of Inspection and Security Staff, and consists of:

1. Presentation of a security motion picture film;

2. A security lecture and discussion of CIA Security Regulations;

3. A short written examination on the subject of the CIA Security Regulations.

7. CHANGE OF STATUS

A. Whenever any changes occur in the personal status of a person attached to CIA, such as marriage, change of address, etc., subsequent to his entry on duty, he will execute, in duplicate, the pertinent Standard Change of Status Report Form, the original copy of which will be forwarded to the appropriate Personnel Division and the duplicate copy to the Chief, Personnel Security Branch, Inspection and Security Staff.

8. EXIT INTERVIEWS

A. TERMINATION OF EMPLOYMENT WITH OR ASSIGNMENT TO CIA. Upon termination of duties with the CIA, all personnel will report to the Personnel Security Branch for an interview with a Security representative, designed to impress upon them their obligations with regard to the maintenance of security of all matters pertaining to the Central Intelligence Agency, and to review the provisions of the Espionage Act and other applicable laws concerning the security of classified information. The interview will include a discussion of what such persons may or may not disclose concerning the duties which they performed while identified with CIA and the functions of the organization. At that time such persons also will surrender all CIA credentials charged to them.

B. LEAVES OF ABSENCE. All persons attached to CIA prior to the start of extended leaves of absence of 60 days or more, will report for interview with a representative of the Personnel Security Branch, during which substantially the same subjects as are mentioned in subparagraph 8. A. above, will be discussed.

9. LEAVE OF ABSENCE - LESS THAN 60 DAYS

Whenever an employee leaves Washington on vacation or official business in which the identification badge is not required, he is urged to turn his badge in to the Physical Security Branch for safekeeping during the period of absence.

[redacted]

XII. SECURITY OF BUILDINGS AND INSTALLATIONS

10. ADMITTANCE OF PERSONS ATTACHED TO CIA AND CERTAIN OTHER GOVERNMENT PERSONNEL. All such persons entering, remaining in, and leaving CIA buildings during regular working hours will be required to display authorized identification credentials, as set forth below:

A. PERSONS REGULARLY EMPLOYED BY, OR ASSIGNED TO CIA, are furnished with numbered photographic badges, as follows:

1. GREEN BORDERED Badge admitting bearer to all CIA buildings.

2. YELLOW BORDERED Badge admitting bearer to all CIA buildings, with the exception of those buildings and areas restricted to holders of Green Bordered Badges. The holder of a Yellow Bordered Badge may enter a Green Badge building or area without a visitor pass by having the receptionist confirm his appointment with the CIA staff member whom he wishes to see. If the appointment is confirmed the receptionist will instruct the guard to admit the Yellow Badge holder, who, upon leaving the building, will be required merely to display his badge.

3. CIA COURIERS AND MESSENGERS are issued Green Bordered Badges with the word "Courier" or "Messenger" stamped on the margin of the Badge photograph.

B. EMPLOYEES OF CERTAIN OTHER GOVERNMENT AGENCIES TEMPORARILY ASSIGNED TO CIA or those who, in the discharge of their official duties, are required to have frequent access to CIA offices, will be furnished, subject to the approval of the Chief of Inspection and Security Staff, with numbered limited photographic passes, bearing issuance dates, expiration dates, names of persons to whom issued and signature of the authorized representative of the Chief of Inspection and Security Staff. Such passes limit admittance of the holders thereof to those CIA buildings or areas specifically described thereon during the periods for which they are issued, unless previously revoked.

C. LOST IDENTIFICATION BADGES. In order to prevent possible compromise of security, it is important that holders of CIA identification badges exercise every precaution to prevent their loss or misuse. A lost badge must be reported at once to the Physical Security Branch, by the person to whom issued, together with a written explanation of the circumstances of loss and efforts made to recover the missing badge. If a person should lose his badge while out of town, he should notify the Physical Security Branch promptly. Normally, a lost badge will not be replaced with a new one for a period of 14 days, during which time every effort should be made to recover the lost badge.

D. ISSUANCE OF BADGES OR SPECIAL CREDENTIALS. Identification badges or special credentials will not be made or issued by any CIA office or organizational unit with the exception of the Physical Security Branch, Chief of Inspection and Security Staff, or the Director of Central Intelligence, who, at his discretion, may authorize the issuance of certain credentials to meet specialized requirements.

E. BADGE LIMITATIONS. The bearers of CIA badges described in subparagraphs A. and B. above, will have access to CIA buildings as indicated, but the possession of a badge does not imply full access to any and all parts of a building. All such persons entering CIA buildings will be subject to such internal security measures as Assistant Directors and Staff Chiefs may prescribe for the areas for which they are directly responsible.

F. PUBLIC BUILDINGS ADMINISTRATION MAINTENANCE EMPLOYEES will be admitted upon displaying proper PBA identification badges issued by that agency. Special workmen will be admitted only by prior arrangement with the Physical Security Branch. All such maintenance employees and special workmen admitted to CIA buildings during regular working hours will be required to sign the guard register upon entering and leaving the buildings.

1. Except in an emergency, the only maintenance workers to be permitted to enter CIA buildings during nonwork hours shall be the members of the char forces and PBA engineers. No exceptions will be made without the prior approval of the Physical Security Branch. All such persons will sign the register at the guard desk upon entering and leaving the building.

2. Staff members of CIA are warned to exercise caution with respect to conversation and exposed classified material when carpenters, electricians, telephone company employees, char people or other maintenance workers are present in their offices. Rooms must not be left unoccupied at such times unless classified material has been locked securely in suitable containers. Any attempt by such persons to overhear conversations or to read classified material should be reported at once to the Chief of Inspection and Security Staff.

G. FORGOTTEN IDENTIFICATION CREDENTIALS. Employees and holders of limited passes who forget their identification credentials will apply to the receptionist for visitor passes in order to gain admittance to their offices. Before issuing such a pass, the receptionist will request that the applicant be identified by his superior or other responsible CIA staff member. The pass will be conspicuously marked "FORGOTTEN BADGE".

[redacted]

H. ADMITTANCE TO BUILDINGS AFTER HOURS. Employees and holders of limited passes who enter CIA buildings after 7:00 P.M. on Mondays through Fridays, or at any time on Saturdays, Sundays and holidays, will sign the guard register upon entering and leaving buildings, in addition to displaying their identification credentials.

11. ADMITTANCE OF VISITORS. Casual or social visitors will not be permitted to enter CIA buildings, and staff members will not request exceptions to this rule. Visitors, as hereinafter referred to, shall be construed to mean persons on official business.

A. VISITOR PASS. All visitors shall be directed to the receptionist and thereafter admitted to the building upon presentation of duly executed visitor passes. A visitor pass will not be issued by the receptionist unless authorized by the CIA staff member concerned with the interview. Upon completion of the visit, the interviewer will sign his name on the pass in ink and indicate the time of the visitor's departure.

B. RECORDS

1. GREEN BADGE BUILDINGS AND AREAS. Each visitor to such buildings and areas will be escorted by the CIA interviewer, or a member of his staff, from the reception desk to his office. Upon completion of the interview the visitor will be escorted back to the reception desk. In addition, if it is necessary for a visitor to call upon two or more interviewers located in different offices within a green badge area, the first interviewer will escort the visitor to the second, etc., and the last interviewer will escort the visitor to the reception desk. Each interviewer will sign his name to the visitor pass and indicate the time of the visitor's departure.

2. YELLOW BADGE BUILDINGS AND AREAS. As a general rule, except during nonworking hours, the escorting of visitors to offices within yellow badge buildings and areas is not required. However, in certain circumstances, escorting of visitors for security or courtesy reasons may be indicated. If an interviewer authorizes the admittance of a visitor with whom he is not acquainted, or if he has doubt regarding the legitimacy of, or necessity for the visit, the interviewer must escort the visitor to and from his office, or between offices, if the visitor is required to see more than one interviewer within the building. The last interviewer will escort the visitor to the reception desk. If an interviewer authorizes the admittance of an unescorted visitor who fails to make an appearance in the interviewer's office after the passage of a reasonable length of time, the latter will take such steps as may be necessary to determine the reasons for the delay. When the receptionist observes an undue interval between the time an

[redacted]

unescorted visitor leaves the interviewer's office and the time he presents himself at the reception desk, the receptionist should make discreet inquiries of the visitor to determine the cause of delay. When the circumstances in such a delay appear suspicious, the receptionist should make a report immediately to the office of the Chief, Physical Security Branch, and to the interviewer of the visitor involved.

C. SURRENDER OF PASS

The visitor pass shall be surrendered to the receptionist as the visitor leaves the building, or to the building guard if the receptionist has left for the day. The guard will turn over all collected visitor passes to the receptionist on the following morning.

D. VISITS DURING OFF DUTY HOURS

A person desiring to visit a CIA office during nonworking hours, including Saturdays, Sundays, and holidays, will be required to execute a special visitor admittance form furnished by the guard after the latter has confirmed the appointment with the CIA staff member. The CIA staff member will sign the form, assuming responsibility for the visitor, and will escort the visitor from the guard desk. Upon completion of the interview, the staff member will escort the visitor from the building, at which time the visitor pass will be surrendered to the guard. The visitor, upon entering and leaving the building, will sign the guard register.

12. RECEPTIONIST STAFF

The Receptionist staff of CIA will be responsible for the courteous reception of visitors; discreet determination of the nature of the visits; arrangement of interviews; issuing visitor passes upon confirmation of appointments with the appropriate CIA staff members; issuing visitor passes to employees who have forgotten their identification credentials; maintaining visitor logs in which are recorded visitors' names and addresses, names and room numbers of persons visited, and the general purposes of the visits; preparing reports related to the Receptionist operations; and will perform such other functions as may be directed by the Chief of Inspection and Security Staff.

13. GUARDS

A. Building Guards furnished by the Public Buildings Administration will admit into CIA buildings only those persons with proper identification credentials authorized for the respective buildings, and visitors to whom visitor passes have been issued.

B. The Guards will patrol the offices after hours for the purpose of checking safes and windows, inspecting tops of desks and other equipment for exposed classified material, and maintain after-hour Guard Registers of visitors and employees who enter CIA buildings after hours or on Saturdays, Sundays and holidays. Security violations detected by the Guards during their patrols will be reported to the Physical Security Branch through the office of the Captain of the Guard.

C. The Guards perform these functions under the security orders and instructions of the Chief of Inspection and Security Staff, through the office of the Captain of the Guard, and all members of CIA are expected to cooperate with the Guards in the performance of their duties.

14. KEYS TO OFFICES

A. Keys to offices will be kept at the Guard desks by the building Guards. Normally, offices will not be locked after regular duty hours. Staff Chiefs may cause to be locked any rooms they deem necessary for security reasons, upon prior approval of the Physical Security Branch. Such rooms will be considered "RESTRICTED AREAS" and only specifically authorized persons will be admitted thereto by the Guards. Persons not regularly assigned to "RESTRICTED AREAS" will not be permitted to enter such areas during regular work hours unless permission is granted by the staff chief of the area concerned.

B. Keys to Restricted Rooms and Areas will be issued to authorized CIA personnel by the PBA Guards only upon written instructions of the Physical Security Branch to the Captain of the Guard. Applications for authorization to draw such keys from the PBA Guards will be made to the Physical Security Branch by the CIA organizational unit concerned. Master keys will not be issued under any circumstances.

IV. SECURITY OF CLASSIFIED DOCUMENTS

15. DEFINITIONS OF CLASSIFICATIONS

A. TOP SECRET: Only that material or information, the unauthorized disclosure of which might cause exceptionally grave damage to the Nation, will be classified TOP SECRET. As a general rule, TOP SECRET matter in

11

time of peace will be limited to that which, if disclosed without authorization, might reasonably be expected to lead directly to a definite break in diplomatic relations, or to a war, or have other exceptionally grave consequences.

Examples: Information or material regarding, or details of discussions or negotiations with, foreign governments on matters of great delicacy.

Information or intelligence material containing indications of sources of intelligence which the United States must protect.

Information or material concerning the existence or details of new devices or methods of warfare of extreme importance to national security.

B. SECRET: Information or material, the unauthorized disclosure of which might endanger national security, seriously jeopardize the international relations of the United States, or endanger the effectiveness of a program or policy of great importance to this Government, will be classified SECRET.

Examples: Information or material regarding, or details of discussions or conferences with high officials of foreign governments on important questions, the premature disclosure of which might seriously affect the foreign relations of the United States.

Reports or acts dangerously unfriendly to the United States, or important trends in foreign affairs greatly endangering national security.

Certain highly important intelligence reports, including reports on subversive activities.

Vital information on important defenses.

High-grade cryptographic devices and related material.

C. CONFIDENTIAL: Information or material, the unauthorized disclosure of which might not endanger national security, but which might prejudice the national interest or the work of any U. S. Government agency by interfering with the development or carrying out of important policy, or by hampering negotiations in progress; might cause serious administrative difficulties; or might result in unwarranted embarrassment of individuals, will be classified CONFIDENTIAL.

Examples: Important intelligence reports.

Reports concerning sabotage or subversive elements, or names of individuals involved.

Investigations, documents and communications of a personal and disciplinary nature, the knowledge of which must be safeguarded for administrative reasons.

D. RESTRICTED: Information or material which does not fall within higher categories, but which should not be communicated outside the Government of the United States without adequate clearance, will be classified RESTRICTED.

Examples: Matters related to internal organizational policy of a secondary character.

Routine internal reports.

Information of a nonconfidential nature, the use of which should be confined to official government activities and should not be publicly disseminated.

16. REGISTERED DOCUMENTS

A. A Registered Document is a document, regardless of security classification, carrying a register number, a copy number, a short title, and instructions that it must be accounted for periodically. Cryptographic devices are also treated as Registered Documents.

B. Documents will be registered only if the originating authority deems it essential to control their distribution in the interests of national security. Approval to register a CIA document must be obtained from the Assistant Director, Office of Collection and Dissemination.

C. Each Registered Document will be conspicuously marked "REGISTERED DOCUMENT" in the upper right-hand corner of the front cover, together with a brief statement reading, "This document must be accounted for periodically."

D. The Short Title of a Registered Document is a code word or a group of Capital letters written together, and usually includes one or more numbers which identify the specific type of document. The Short Title must not reveal the subject content of the Registered Document.

E. A communication including both the Short Title and the full title of a Registered Document must be given the same security classification as the Registered Document.

[redacted]

F. Custodians of Registered Documents are designated and are charged with duties as follows:

1. The CIA Custodian of Registered Documents and the Alternate Custodian, designated by the Director, CIA, maintain the record of the custody and provide the office of record for all copies of Registered Documents in the Agency.

2. A Navy Registered Documents Custodian, designated by the Naval Administrative Command, CIA, maintains the record of custody of all Navy Registered Documents in CIA. The Navy Registered Documents Custodian is also designated as an Area Custodian of Registered Documents for CIA to maintain control over Navy and CIA Registered Communications Publications, Documents and Devices.

3. Area Custodians of Registered Documents are nominated by Assistant Directors and Staff Chiefs to the CIA Custodian of Registered Documents as the need for such appointments arise. Nominees shall not be permitted to act as Area Custodians until their nominations have been confirmed by the CIA Custodian of Registered Documents and the Chief, Inspection and Security Staff. All nominees must also be designated as Alternate Top Secret Control Officers.

G. Registered Documents (other than those listed in paragraph F. 2. above) will be receipted for and distributed within CIA only by the CIA Custodian of Registered Documents or the Alternate Custodian. Any member of CIA who desires a Registered Document will request the originating agency to forward it through the CIA Custodian.

H. Custody of a Registered Document may be transferred by the CIA Custodian of Registered Documents to an Area Custodian who shall assume responsibility for the document and render periodic reports as required.

I. CIA Registered Documents, transferred in quantity by the CIA Custodian of Registered Documents to an outside agency, may be dropped from periodic accountability to CIA. The "Transfer of Registered Documents" form will be stamped as follows:

"Accountability to be assumed by receiving agency in accordance with rules governing his service. Periodic accountability to CIA not required."

17. AUTHORITY TO DETERMINE CLASSIFICATION

Documents and correspondence will be classified according to the provisions of paragraph 15, Section IV. The responsibility for

insuring that documents produced in CIA are classified properly rests with Assistant Directors or staff personnel occupying comparable positions, who will establish adequate procedures within their offices or staffs to provide for review of classifications given documents by their subordinate officials, in order to insure that correct and uniform classification standards are applied. Overclassification must be avoided, for such practice will tend to weaken the entire security classification structure.

10. CLASSIFICATION MARKING OF MATERIAL

A. TOP SECRET DOCUMENTS

1. All Printed Top Secret Documents will have the classification printed thereon, in so far as is practicable in red, with the size of the type noticeably larger than that of the text. The classification will appear on the top and bottom of the front cover or first sheet, on all succeeding pages, and on the back of the cover sheet or last page. The classification markings shall be spaced at least ½ inch from the top and bottom of the text.

2. When Top Secret Documents Are Typed, the classification will be marked on all pages and copies thereof, top and bottom, by means of a red inked rubber stamp, the type of which is noticeably larger than that of the typewritten text.

3. Top Secret Documents Prepared By Means Of Stencils Or Ditto Masters will be reproduced on paper with the classification pre-printed in red, top and bottom, on the front cover or first sheet, and on all succeeding pages. The classification on the back of the rear cover or last page either may be pre-printed or marked by means of a conspicuous red inked rubber stamp. The pre-printed classification marking will be noticeably larger than that of the text and will be spaced at least ½ inch from the top and bottom of the text.

B. SECRET, CONFIDENTIAL AND RESTRICTED DOCUMENTS

1. Such Documents When Printed, will have the classification printed thereon, the color of which may be the same as that of the text. The classification marking will be in type noticeably larger than that of the text, and will appear on the front cover or first sheet, and on all succeeding pages. The classification marking will be spaced at least ½ inch from the top and bottom of the text.

2. Such Documents When Typed, will have the classification marked on all pages and copies thereof, top and bottom, by means of a red inked rubber stamp, the type of which is noticeably larger than that of the typewritten text.

3. Such Documents When Prepared By Means of Stencils Or Ditto Masters, may have the classification cut thereon, top and bottom, on each sheet. The classification marking will be spaced at least ½ inch from the top and bottom of the text and will correspond with the following design in underscored capital letters:

S-E-C-R-E-T

CONFIDENTIAL

RESTRICTED.

In lieu of cutting the classification on the stencil or ditto master, the classification may be recorded on all pages of Secret, Confidential and Restricted documents by means of a red inked rubber stamp of conspicuous size.

19. SAFEGUARDING OF CLASSIFIED DOCUMENTS AND MATERIAL

A. Storage of classified documents and material (including stenographic notes, work sheets, carbon paper and stencils).

1. Top Secret, Secret, Confidential and Registered Documents of All Classifications, will be stored in safes or fire resistant safe-type file cabinets with not less than 3-way built-in combination locks.

2. Restricted Documents Not Registered should be stored in ordinary steel lock file cabinets.

3. Armed Guard. In certain unusual circumstances, or if for operational reasons, it is not possible to apply the foregoing storage requirements, arrangements may be made, subject to the approval of the Chief of Inspection and Security Staff, to safeguard the documents temporarily under armed guard, when not in use.

4. Carbon Papers, Stencils, Stenographic Notes and Work Sheets. Used carbon papers, until no longer serviceable, will be stored in safes when not in use. Unserviceable carbon papers will be torn in small pieces and placed in the classified waste receptacle. Such papers shall not be discarded in waste baskets. Used carbon papers shall not be kept in desks, desk trays, etc., during non-working hours. Classified stencils, until disposed of in the classified waste, will be stored in safes. The same applies to stenographic notes, work sheets and the like.

5. Calendar Pads and List Finders, although not in themselves classified, frequently contain information of considerable security significance. Such articles, therefore, should be locked in safes during non-working hours.

B. GENERAL

The safekeeping of classified documents is of prime importance. The foregoing storage requirements, prescribed for the various security classifications, must be adhered to strictly. Documents classified above RESTRICTED will not be kept in locked desks or other unauthorized containers, nor will they otherwise be left unprotected at any time. It is strictly prohibited to take home for any purpose whatsoever, material classified above the level of "RESTRICTED". All work thereon must be performed in the office where it can be protected fully. Precautions should be taken to prevent unauthorized persons from seeing classified documents while work is being performed on them.

20. SAFES

A. Each combination safe and safe-type file cabinet will have a sticker applied inside the container on which will be recorded the name of the person responsible for the safe, his home address and telephone number, the names, home addresses and telephone numbers of all other persons in possession of the combination, listed in the order of principal use, and the date when the combination was last changed. The sticker will be placed on the side and near the front panel of each drawer of the conventional safe-type file cabinet, and on the inside of the door of the door-type safe. Scotch tape should be placed over the sticker to secure it properly.

B. The person responsible for a safe is also accountable for its proper working condition. He should arrange with the Physical Security Branch for the immediate repair of any defective safekeeping equipment in his custody.

C. Combinations of safes and safe-type file cabinets will be known only to those persons who are required to have access to them in the performance of their official duties. Combinations of all safekeeping equipment will be changed at least once every six months. If a person having knowledge of the combination of a safe should leave the organizational unit or CIA, the combination of the safe involved will be changed immediately. It is the responsibility of custodians to have the combinations changed in accordance with these requirements. A representative of the Physical Security Branch will make the change upon request by the custodian. The Physical Security Branch alone will change the combinations of CIA safes, unless an exception is granted specifically by the Chief of Inspection and Security Staff.

D. When a safe is delivered to an office, no classified material will be stored therein until the combination of the safe first has been changed.

E. A number will be assigned to each safe by the Physical Security Branch. The person responsible for a safe or safe-type file cabinet will turn the combination of the safe over to the Physical Security Branch, double-wrapped in a sealed envelope (inner envelope marked "TOP SECRET"), signing his name on the flap of the outer envelope. The combination of a safe may be obtained from the Physical Security Branch by the person whose signature appears on the flap of the envelope or by his staff chief, upon proven necessity and receipt therefor. A safe combination never will be divulged over the telephone, except in an extremely grave emergency, following which the combination will be changed promptly.

F. It will be the responsibility of the custodian of safes to ascertain the proper method of locking all types of safes in his or her custody prior to use. The same responsibility applies to Staff Duty Officers prior to making their first security checks.

G. Upon locking a safe, an "Open Sign" will be placed in the top handle of the multiple-drawer safe or on the handle of the door-type safe, and will not be removed until after the safe has been secured at the close of the day.

21. DISPOSITION OF CLASSIFIED WASTE.

A. Preliminary drafts, copies, carbons, stencils, stenographic notes, work sheets, and the like, pertaining to classified matter of all classifications, will be torn or shredded into small pieces, and placed in envelopes or other receptacles unequivocally marked "SECRET". Custodians will dispose of their classified waste by placing it in classified waste sacks maintained for that purpose at the guard posts located at the main entrances to CIA Buildings or Areas. The classified waste sacks are picked up daily by the Physical Security Branch and disposed of by burning. Classified waste, until disposed of in the sacks at the guard posts, will be safeguarded by the custodians thereof in the same manner as SECRET documents.

B. Waste baskets will be used for unclassified waste only.

22. DESTRUCTION OF CLASSIFIED DOCUMENTS

A. The destruction of classified documents must be accomplished in accordance with existing law and regulations. The law provides that government records may not be destroyed without the approval of the Archivist of the United States and the Congress of the United States. Custodians of documents will survey periodically all such

material in their possession and, if deemed of no further use, will request their Area Records Officer to review the documents and give directions for appropriate disposition as provided in the CIA regulations on Records Management.

B. TOP SECRET DOCUMENTS, NOT REGISTERED, will be destroyed by burning by the custodian thereof or his designee at the CIA incinerator. The custodian or his designee will remain at the incinerator until all the documents have been burned completely. The appropriate Area, Alternate or Assistant Top Secret Control Officer must be notified of the destruction in order that the proper entries may be made on the Top Secret Log. When a Top Secret document is destroyed, the disposal certificate portion of the Signature Record and Cover Sheet, attached to the document, will be executed. The cover sheet will then be forwarded to the CIA Top Secret Control Officer, through the appropriate Area Top Secret Control Officer. Subparagraphs A. and I. of this section also must be complied with.

C. SECRET, CONFIDENTIAL AND RESTRICTED DOCUMENTS, NOT REGISTERED, may be destroyed by burning by the custodian thereof or his designee at the CIA incinerator, or such documents may be shredded or torn into small pieces and placed in the classified waste receptacle, for subsequent burning by the Physical Security Branch. Under no circumstances will whole documents be placed in the classified waste receptacles. Subparagraphs A. and I. of this section also must be complied with.

D. REGISTERED DOCUMENTS, will be destroyed by burning, by the Area Custodian of Registered Documents, or his designee, at the CIA incinerator. Such person will remain at the incinerator until all the documents have been burned completely. Before a Registered document may be destroyed, authorization must be obtained by the Area Custodian (with the exception of the Communications Division) from the CIA Custodian of Registered Documents. With respect to Registered Top Secret Documents, all requirements pertaining to the destruction of Unregistered Top Secret Documents, as set forth in subparagraph B. above, must be observed also. In addition, subparagraphs A. and I. of this section also must be complied with.

E. CLASSIFIED DOCUMENT RECEIPTS. CIA Document Receipts which reflect the issue and receipt of specific classified documents may be destroyed, in accordance with the provisions of subparagraph C. above, as follows:

1. Top Secret and Registered Document Receipts, after five years.

2. Unregistered Secret, Confidential and Restricted Document Receipts, after two years.

F. CIA COURIER RECEIPTS which reflect the receipt and delivery of packages containing classified documents may be destroyed after one year in accordance with the provisions of subparagraph C. above.

G. BURN TEAMS. Chiefs of Offices, Staffs and Divisions may, if they wish, organize "burn teams" for the purpose of destroying documents in accordance with the provisions of subparagraphs A-B-C-D-E-F above. Central collecting points for documents to be destroyed by the "burn teams" may be established in offices or areas.

H. PERSONS ASSIGNED TO BURN CLASSIFIED DOCUMENTS

Office Chiefs will assure themselves that persons assigned to such duties in accordance with the provisions of this instruction, are dependable and thoroughly familiar with the security requirements involved. Such persons need not be of any minimum grade or rank.

I. CERTIFICATES OF DESTRUCTION

1. For All Unregistered Top Secret Documents, and Unregistered Documents of All Other Classifications, Which Must be Accounted for to the Originating Office or Agency by Specific Instructions, a Certificate of Destruction will be executed, in duplicate, and signed by the custodian. The Certificate will include, in addition to the signature of the custodian, the date, name of organizational unit, and a list of the documents and their classifications. A witness to the destruction will not be required. Document Receipts for Top Secret documents, when destroyed after the required retention period, will not be listed on a Certificate of Destruction. The original copy of the Certificate of Destruction will be sent to the Records and Files Section, Central Records Branch, OCD.

2. For Unregistered Secret, Confidential and Restricted Documents, Which Carry No Specific Accountability Requirements to the Originating Office or Agency, a Certificate of Destruction for records management purposes, will be prepared in duplicate and signed by the custodian. The Certificate will include, in addition to the signature of the custodian, the date, name of organizational unit, identification and security classifications of the file series destroyed, and the volume of the documents in approximate linear inches or feet. The volume of the material listed on the Certificate of Destruction will include the documents destroyed by burning and those disposed of in the classified waste. A witness to the destruction is not required. The original copy of the Certificate of Destruction will be sent to the Records and Files Section, Central Records Branch, OCD.

3. Registered Documents. Certificates of Destruction for all Registered Documents of all classifications, will be prepared in the same manner as that prescribed in subparagraph I-1 above, with the exception that the original copy of the Certificate will be forwarded to the CIA Custodian of Registered Documents.

23. RESTRICTIONS ON DISSEMINATION OF CLASSIFIED INFORMATION

A. C.I.A. members will refrain from giving unauthorized persons any classified information about their work. Public or private discussion of classified data with, or in the presence or hearing of, any person not authorized to have knowledge thereof, is strictly forbidden. This prohibition also applies to friends and members of the families of persons attached to CIA, when such individuals are not entitled officially to knowledge of classified information.

B. Any person on duty with CIA who, with deliberate intent or through gross negligence, causes classified information affecting the national security to be conveyed to an unauthorized person is subject to the penalties provided for by the Espionage Act.

C. The following description of the Central Intelligence Agency is common knowledge and CIA members, unless prohibited by their superiors from publicly associating themselves with CIA for security or other reasons, may quote therefrom when it is deemed necessary:

> "The Central Intelligence Agency is an independent government agency established under the National Security Council. It coordinates the foreign intelligence activities of the several departments and agencies of the government in the interest of national security and advises the National Security Council in matters concerning such intelligence activities as relate to national security."

No amplification of the foregoing statement to unauthorized persons will be permitted.

D. No person is entitled, solely by virtue of his grade or position, to knowledge or possession of classified matter or information. Such matter and information shall be restricted only to individuals whose official duties require such knowledge or possession.

24. LOSS OR COMPROMISE OF CLASSIFIED DOCUMENTS

In case of loss or compromise of classified documents or information, immediate notification thereof will be made to the Chief of Inspection and Security Staff.

25. CLASSIFICATION ADVERTENCE

A. Office and Staff Chiefs or their designees should periodically review classified documents in the custody of their respective organizational units, with a view to cancelling or downgrading the classifications

of these documents, the security significance of which has diminished or ceased to exist. The person making the original classification, his successor or superior, may cancel or modify the classification of a document, by reason of changed conditions or over-classification, by striking out the classification at the top of the cover or first page and recording the following information:

Central Intelligence Agency

Classification

Cancelled

Changed to _____

By Authority of

Name _____

Office _____

Date _____

B. Rubber stamps for this purpose may be obtained from the Physical Security Branch through the Area Security Officers.

C. In the course of review, consideration should also be given to the upgrading of documents which occasionally will be found to have been assigned inadequate classifications.

D. In cases wherein appropriate authority to effect changes in classification is not readily determinable or available, questions of policy and procedure may be referred to the Security Control Staff, Chief of Inspection and Security Staff.

E. When the classification of a document is altered, steps should be taken, in so far as is practicable, to change the classification of all copies thereof correspondingly. Offices of origin, when changing the classifications of documents, should so inform all persons to whom such documents had been distributed, if the recipients thereof are readily determinable.

26. DUPLICATING OR ABSTRACTING OF CLASSIFIED DOCUMENTS

A. Duplication of classified material by the originating office shall be limited to the minimum number of copies necessary for efficient operation.

B. Classified documents will not be duplicated without authorization of the originating CIA office or outside agency.

C. Abstracts of classified documents may be made with the approval of the originating CIA office or outside agency. The abstract, however, will not necessarily bear the same classification as the document from which it was taken, but will be classified on its own merits, with the concurrence of the office or agency which originated the document.

D. The originating office will maintain a record of the distribution of classified material, including the names of the recipients and the number of copies assigned to each.

27. CONTROL OF TOP SECRET DOCUMENTS, INCLUDING REGISTERED TOP SECRET DOCUMENTS. (For detailed instructions see Regulation [redacted] 25X1A

A. It is a primary responsibility of all CIA personnel to insure that each Top Secret document, registered or unregistered, is handled in a secure manner and that unauthorized persons may in no instance have access to such documents.

B. Every copy of each Top Secret document prepared or received by any activity or member of CIA must be recorded by the Central Top Secret Control or by the Area Top Secret Control serving the activity preparing or receiving the document. Each copy will be assigned a control number and a copy number and will be recorded in the Standard Top Secret Log or other recording medium approved jointly by the CIA Top Secret Control Officer and the Chief, Physical Security Branch.

C. Every copy of a Top Secret document retained within CIA offices will be covered at all times by a Signature Record and Cover Sheet. The Cover Sheet attached to a Registered Top Secret document must be marked conspicuously "Registered Document". Each CIA member who reads or learns the contents of a Top Secret document will sign his name on the Cover Sheet.

D. The Central Top Secret Control is established in the Central Records Branch, Library Division, OCD. It serves as the central office of record for the Agency and provides the archives for Top Secret documents.

E. A CIA Top Secret Control Officer designated by the Director, CIA, exercises functional supervision over all Agency Top Secret Control measures.

F. Area Top Secret Controls, serving as offices of record for organizational segments of CIA, are established by joint agreement of the CIA Top Secret Control Officer and Assistant Directors of Offices or Chiefs of Staffs. Each such area will be headed by an Area Top Secret Control Officer designated by the CIA Top Secret Control Officer. Alternate and Assistant Top Secret Control Officers serve under the Area Top Secret Control Officers.

G. Area, Alternate, and Assistant Top Secret Control Officers, and Top Secret Couriers who are also Alternate Top Secret Control Officers, are nominated by Assistant Directors and Staff Chiefs to the CIA Top Secret Control Officer. Nominees shall not be permitted to act as Control Officers until their nominations have been confirmed by the CIA Top Secret Control Officer and the Chief, Inspection and Security Staff.

H. The CIA Top Secret Control Officer and Area and Alternate Top Secret Control Officers are the only persons who shall be permitted to transmit and receipt for Top Secret material moving between CIA and outside agencies.

I. Assistant Top Secret Control Officers, in addition to those named in the preceding paragraph, are the only persons who shall be permitted to transmit and receipt for Top Secret material moving within CIA.

J. Chiefs of Offices and Staffs are responsible for the designation of persons in their own offices, other than Alternate and Assistant Top Secret Control Officers, whom they deem are operationally required to see Top Secret material, and they are further responsible for insuring that necessary controls are exercised to confine the number of such persons to the minimum.

K. The Chief, Inspection and Security Staff, may conduct periodic and unannounced checks of offices of CIA to determine whether the regulations pertaining to TOP SECRET material are being observed.

28. TRANSMISSION OF CLASSIFIED DOCUMENTS OUTSIDE CIA

(For detailed instructions see Regulation [redacted] 25X1A

A. TOP SECRET DOCUMENTS, NOT REGISTERED, will be double wrapped when transmitted by Top Secret Couriers, who also are Alternate Top Secret Control Officers. Such documents need not be double wrapped when hand delivered by the CIA Top Secret Control Officer, Area Top Secret Control Officers, or Alternate Top Secret Control Officers, other than Top Secret Couriers. Document Receipts will always be obtained for TOP SECRET Documents, unless transmitted by approved electrical means. The recipient's signature in the sender's Top Secret Log Book may be substituted for the Standard Document Receipt Form. Only Top Secret Couriers or approved electrical means will be utilized for the transmission of TOP SECRET Documents, unless hand delivered by the Control Officers specifically mentioned above. When transmission is accomplished by such hand delivery, the appropriate Area Top Secret Control Offices must be notified. Under no circumstances may TOP SECRET Documents be transmitted by Registered Mail.

B. SECRET AND CONFIDENTIAL DOCUMENTS, NOT REGISTERED, will be double wrapped, unless hand delivered by the custodians thereof. Document Receipts will be obtained for SECRET Documents, but not for CONFIDENTIAL Documents, unless the sender deems it necessary. The recipient's signature in the sender's SECRET and CONFIDENTIAL Log Book may be substituted for the Standard Document Receipt Form. Only authorized couriers, approved electrical means or Registered Mail will be utilized for outside transmission of SECRET and CONFIDENTIAL documents, unless hand delivered by the custodians thereof.

C. RESTRICTED DOCUMENTS, NOT REGISTERED, may be delivered by messenger, any office assistant, or by regular mail. Such documents need not be double wrapped, nor is it necessary to obtain document or envelope receipts for them.

D. REGISTERED DOCUMENTS

1. REGISTERED TOP SECRET Documents will be transmitted in the same manner as Unregistered Top Secret Documents, with the exception that Registered Documents Transfer Reports will be substituted for the Standard Document Receipt Forms.

2. REGISTERED SECRET, CONFIDENTIAL AND RESTRICTED DOCUMENTS will be transmitted in accordance with the procedure prescribed for UNREGISTERED SECRET Documents, with the exception that Registered Documents Transfer Reports will be substituted for Standard Document Receipt Forms.

3. A REGISTERED Document may not be transferred from one area custodian to another area custodian, or to an activity outside of CIA, except through the CIA Custodian of Registered Documents.

29. TRANSMISSION OF CLASSIFIED DOCUMENTS WITHIN CIA

(For detailed instructions see Regulation [redacted] 25X1A

A. TOP SECRET DOCUMENTS, NOT REGISTERED, will be double wrapped when transmitted by Top Secret Couriers, who also are Alternate Top Secret Control Officers. Such documents need not be double wrapped when hand delivered by the CIA Top Secret Control Officer, or by Area, Assistant and Alternate Top Secret Control Officers, other than Top Secret Couriers. When transmission is accomplished by such hand delivery, the appropriate Area Top Secret Control Offices must be notified. Document Receipts will be obtained in all cases. The recipient's signature in the sender's Top Secret Log Book may be substituted for the Standard Document Receipt Form. No persons other than those specifically mentioned above, shall be permitted to transmit TOP SECRET Documents within CIA.

[redacted]

B. SECRET AND CONFIDENTIAL DOCUMENTS, NOT REGISTERED, will be enclosed in chain envelopes (no further cover required) and sealed by means of a CIA gummed label, only when delivery is made by couriers or messengers. The envelope will bear no marking to indicate the classification of its contents. Double wrapping may be substituted for the chain envelope, if the sender deems additional precautions advisable. Document Receipts will be obtained only when the sender considers it desirable. The recipient's signature in the sender's Log Book may be substituted for the Standard Document Receipt Form, when a receipt is required by the sender. Authorized couriers, custodians or any responsible office assistant may make deliveries of SECRET and CONFIDENTIAL Documents, either between or within CIA buildings. Messengers shall be permitted to deliver such documents only within CIA buildings.

C. RESTRICTED DOCUMENTS, NOT REGISTERED, may be delivered by any person attached to CIA. When the messenger service is utilized, the document will be enclosed in a chain envelope (no further cover required). The envelope need not be sealed and will bear no marking to indicate the classification of its contents. Document or envelope receipts are not required.

D. REGISTERED DOCUMENTS

1. REGISTERED TOP SECRET Documents will be transmitted in the same manner as UNREGISTERED TOP SECRET Documents, with the exception that Registered Documents Transfer Reports will be substituted for the Standard Document Receipt Forms.

2. REGISTERED SECRET, CONFIDENTIAL AND RESTRICTED Documents will be transmitted in accordance with the procedure prescribed for UNREGISTERED SECRET Documents, with the exception that Registered Documents Transfer Reports will be substituted for the Standard Document Receipt Forms.

3. A REGISTERED DOCUMENT may not be transferred from one area custodian to another area custodian, except through the CIA custodian of Registered Documents..

30. MAINTENANCE OF LOGS

A. TOP SECRET LOGS. Alternate or Assistant Top Secret Control Officers shall be responsible for the maintenance of Top Secret Logs, both locally and in the field. The Logs will list all Top Secret material, both Unregistered and Registered, received and dispatched at all of the Top Secret Control Areas.

B. SECRET and CONFIDENTIAL LOGS will be maintained by responsible persons designated specifically for that purpose by Office or Division Chiefs. All Secret and Confidential material, not Registered, will be logged in at the initial point of receipt in an Office or Staff, normally at the Division level (except in the smaller Divisions), and will be logged out at the final point of dispatch when bound for destinations outside of the Office or Staff level or when dispatched to a field office or between subdivisions of an office located in different buildings. Organizational units not included in the foregoing may maintain Logs when deemed desirable for operational reasons or because of the nature of the activity involved. Field offices will maintain Logs of all Secret and Confidential material received and dispatched by them. If, during the course of operations, it is necessary or expedient at times to hand carry Secret or Confidential documents, the control points at each end must be notified.

C. RESTRICTED DOCUMENTS, NOT REGISTERED, need not be logged, but the custodians thereof will be held responsible for such documents with respect to accountability. If an organizational unit elects to log Restricted material, the recordings may be made on the Secret and Confidential Log or on a separate log.

D. REGISTERED DOCUMENT LOGS will be maintained by Area Registered Document Custodians for all Registered Secret, Confidential and Restricted documents.

E. LOGS WILL BE MAINTAINED ON STANDARD FORMS or other recording media approved jointly by the CIA Records Officer and the Chief, Physical Security Branch.

V. GENERAL SECURITY PRACTICES

31. SECURITY IN OFFICE ROUTINE

A. Since effective security is largely a matter of habit, each office must be run on a set routine designed to insure complete security. Daily operations should be performed in such a manner that security at no time will be compromised.

B. Telephone

1. The presumption must be that every conversation by telephone or inter-office communication system will be overheard by unauthorized persons. No wires are protected, not even those carrying inter-office calls. Therefore, TOP SECRET, SECRET, or CONFIDENTIAL information must never be discussed over such facilities.

2. When answering the telephone, an employee will give the name of the person whose office is called, e.g., "Mr. Smith or Mr. Smith's office", or he may give the telephone extension only. In certain areas special telephone instructions may be issued by the Chiefs of the Offices involved. Switchboard operators will answer [redacted] to calls from outside CIA, with the exception that they will answer "Central Intelligence Agency" to incoming calls on dial code lines. When a person requests information over the telephone and there is any doubt regarding his identity or the necessity of his requiring the information, the employee will take his name and telephone number and offer to return the call. The employee will then discuss the request with his superior and decide upon a reply. Employees will not transmit information about CIA to unknown or unauthorized persons.

25X1A

G. SAFES. A large sign marked "OPEN" will be inserted in the handle of the top drawer of each safe-type file cabinet and on the handle of each door type safe during the time such equipment is unlocked. This is intended as a visual warning to custodians or other office employees to lock safes at the end of the day or during unguarded periods within the regular work day.

D. UNOCCUPIED ROOMS. Employees will not leave rooms unoccupied at any time during the day if classified documents are exposed in the office. If it is necessary to leave a room unoccupied, all material classified above "RESTRICTED" first must be locked securely in the proper safekeeping equipment or temporarily placed in another employee's custody. During such periods, classified documents will not be placed in desks, or under trays or desk pads. The locking or bolting of a door to an unoccupied room while classified information is exposed therein, is contrary to security requirements unless the interior of the room is under the constant observation of employees in adjacent rooms.

E. VISITORS. No employee will permit classified papers to be exposed on his desk in such a fashion that they could be read by persons visiting his office who are not authorized to have such information. At such times classified material should be turned face down on the desk.

F. CLASSIFIED WASTE. Classified waste must be disposed of in accordance with the regulations governing the disposition of such matter. Waste baskets will not be utilized for that purpose.

G. DEFECTIVE STORAGE EQUIPMENT. Employees immediately will report defective safekeeping equipment to the Physical Security Branch which will arrange to have the necessary repairs made. In the meantime, classified material should be transferred from the faulty containers to properly functioning, appropriate safekeeping equipment.

[redacted]

H. SECURING OFFICE AT END OF DAY. Each member of CIA will take the following steps to insure the security of his area before departing for the day:

1. Clear the top and inside of desk of all material classified above RESTRICTED and lock it in safe. Determine that all such material in other parts of the office has been secured in a safe.

2. Invert empty "In" and "Out" trays, or turn them on their sides.

3. Determine that classified waste has been disposed of properly or is locked in safe.

4. Lock Safes. In locking the safe-type file cabinet, first close each drawer completely. Then rotate the dial at least three complete, consecutive revolutions in one direction and at least three complete, consecutive revolutions in the opposite direction. Then check each drawer of the safe by firmly depressing the thumb latch and at the same time vigorously pushing the drawer inward and pulling it outward several times. In locking the door type safe or a vault door, rotate the dial as indicated above, firmly turn the handle of the safe back and forth, and simultaneously pull outward on the door.

5. When the safes have been secured, the custodians or users thereof will execute the security check sheet attached to the top or side of each safe and safe-type file cabinet, indicating that the equipment has been locked properly.

6. As a double check, the last person to leave the room will make certain that the above security measures have been taken, that the windows are locked and the lights extinguished.

3P. SECURITY OUTSIDE OF OFFICE

A. DISCUSSION OF CIA ACTIVITIES. Employees will not discuss their work or the activities of CIA with anyone outside of the office, except as may be required in the performance of their official duties.

B. TALKING IN PUBLIC PLACES. Particular caution should be exercised in refraining from discussing classified information in restaurants, at social gatherings, on public conveyances or other such places.

C. CREDIT REFERENCE.

1. Subject to the restrictions of subparagraph C-2 below, employees may use CIA as a credit reference. Information which

employees may furnish in this connection will be limited to the following:

Personnel Office
Central Intelligence Agency
2430 "E" Street, N. W.
Washington 25, D. C.

Employees will not furnish the names of their superiors or other members of CIA, or units of organization, for credit reference purposes.

2. In some areas of CIA, by reason of the nature of the duties performed by certain employees, the use of CIA for credit reference purposes may be prohibited by the Chiefs of the Offices concerned.

D. TRAFFIC ACCIDENTS, ARRESTS, COURT PROCEEDINGS. If an employee should become involved in a traffic accident, court proceedings or other external affair in which CIA might become involved directly or indirectly, even though the matter be almost entirely personal in nature, he should report the affair to the Physical Security Branch at the earliest opportunity in order that suitable security measures may be taken if circumstances warrant.

E. GROUP SOCIAL ACTIVITIES. In the interest of security, group social activities of CIA personnel, such as annual parties, picnics, dances and athletics, will not be identified with CIA, directly or indirectly.

33. STAFF SECURITY CHECK

A. Each office chief will form a Staff Duty Officer Organization to conduct a daily, final after-hour security checks of the area occupied by that staff. The Staff Duty Officers may be rotated, on a daily, weekly or similar basis, and will be selected from among the members of the office staff. A schedule will be prepared in advance by the office chief or his designee, indicating the day or days that each Staff Duty Officer will perform the after-hour security check. Caution should be exercised so that no one Staff Duty Officer will have too large an area assigned to him.

B. It shall be the responsibility of office chiefs or their designees to instruct Staff Duty Officers in the proper performance of their security checks prior to their commencing such duties.

C. The Staff Duty Officer will begin his security check at the end of the regular work day when all or most of the employees have left. During the course of the security checking process, the Staff Duty Officer will execute a check list, which will include the listing of any security violations, defective equipment, security hazards, etc.,

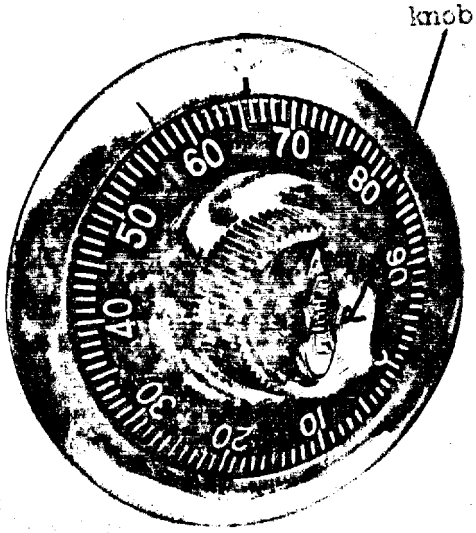
detected by him. All such matters detected by the Staff Duty Officer should be referred by him to the office or staff security officer for appropriate action.

D. If, during the course of the security check, an employee is working late, the Staff Duty Officer will inform him that he will be held responsible for the security of his own immediate room or area, and the Staff Duty Officer will so note on his check list. The check lists will be forwarded to the Physical Security Branch on the following day, through the office or staff security officer.

E. The Staff Duty Officer, in the performance of his security check, will insure that:

1. All safes and all safe-type file cabinets are locked, including all drawers of the safe-type file cabinets. In checking the safe-type file cabinet, rotate the dial at least three complete, consecutive revolutions to the left only. Then check each drawer of the safe by firmly depressing the thumb latch and at the same time vigorously pushing the drawer inward and pulling it outward several times. In checking the door type safe or vault door, rotate the dial at least three complete, consecutive revolutions to the left only, firmly turn the handle of the safe back and forth, and simultaneously pull outward on the door.

IMPORTANT NOTE. Dial equipped with a knob in its center. (See illustration below.) If, in checking this type of lock, the dial catches before it can be rotated at least three times to the left as specified in subparagraph E-1 above, then rotate the dial three times to the right. If the dial catches again, press firmly downward on the thumb latch of the drawer on which the dial is located and pull outward. The drawer probably will then open, indicating that the custodian had not secured the safe properly.



2. No material classified above RESTRICTED, including used carbon paper, stencils and the like, has been left exposed on desks, safes or other office equipment, in desk trays, on the office floor, or on the walls.

3. All classified waste has been secured properly.

4. Doors to restricted rooms and areas are secured properly.

5. Windows are locked.

6. Lights are extinguished.

34. NIGHT SECURITY OFFICERS

A. A staff of Night Security Officers is attached to the Physical Security Branch, Chief of Inspection and Security Staff, the members of which perform certain security functions during all non-working hours Mondays through Fridays, and 24 hours on Saturdays, Sundays and holidays.

B. The Night Security Officers conduct after-hour security inspections of CIA installations; make security checks of safes and offices; inspect the insides of desks for improperly stored classified material; perform specialized technical security functions; resolve security problems which arise after hours; are charged with the responsibility of performing certain duties in cases of emergency which may occur after hours, in accordance with the provisions of the CIA Disaster Plan; discharge special security assignments; and prepare reports related to the foregoing activities.

35. OFFICE, STAFF AND DIVISION SECURITY OFFICERS

A. In order to lend effective implementation to the CIA Security Program, each Assistant Director and Staff Chief, will appoint a Security Officer to be responsible to him for insuring compliance with CIA Security Regulations and Policies by the members of the Staff within his organizational jurisdiction. In some areas, because of the type of organizational structure or physical separation, it may be desirable to appoint Security Officers at the Division level. The Security Officers must be Officers or responsible civilian employees in grade GS-9 or higher.

B. Assistant Directors and Staff Chiefs will forward the names of Security Officers appointed by them, to the Chief of Inspection and Security Staff, who will also be notified of changes in Security Officers, as they occur.

C. Security Officers appointed under this requirement will maintain liaison with the appropriate operations of the Chief of Inspection and Security Staff.

36. PHYSICAL PENETRATION, CIA AREAS OR INSTALLATIONS. If a member of CIA discovers evidence or indications of forced penetration of a CIA building, area or safekeeping equipment, he will take the following action at once:

A. Secure the room or area and arrange for an office employee to stand guard in order to prevent any person from entering.

B. Refrain from touching or disturbing the equipment, documents, building features or any tools involved.

C. Call the Chief of Inspection and Security Staff, and await arrival of a Security representative.

37. SECURITY VIOLATION PENALTY SYSTEM

A. Members of CIA charged with Security Violations, are subject to the following administrative penalties: 25X1A

[redacted]

B. The above guide will not be a bar to immediate termination of employment due to any security violation considered sufficiently serious to warrant such action.

C. These penalty provisions shall apply to personnel detailed to duty with CIA from other government agencies except that the relief of such an individual from further duty with CIA and return to his parent agency will be recommended in lieu of suspension or termination of employment.

D. If the first violation occurs on a date more than two years after an individual first enters on duty with CIA, the particular provisions of paragraph A.1.a. above shall not be applied.

E. If an individual serves two continuous years without being charged with a security violation, any or all violations which he committed prior to the commencement of said two year period shall be stricken from the records, in so far as the application of these administrative penalties is concerned.

38. CIA DISASTER PLAN

A. A Disaster Plan has been developed for the protection of CIA classified information, installations and personnel in the event of fire, natural disaster, attempted physical penetration, or other emergency, during or after regular work hours.

B. The Disaster Plan Organization is headed by a Chief of Emergency and a staff of Emergency Officers who are charged with the responsibility of performing specific duties during emergencies.

C. In the various offices of CIA, notices are posted which set forth the action to be taken by all persons attached to CIA, when an emergency occurs.

VI. SECURITY OF FIELD INSTALLATIONS

39. In so far as possible, all physical security measures contained in this manual shall also apply to field installations. It is realized, however, that local conditions, the nature of the work being performed, and other considerations may warrant change in, or deviation from, some of the procedures and requirements set forth herein. Field installations and activities which do not lend themselves to these security regulations in their entirety, will be governed by special security directives, regulations and instructions.