

Security Manuals
12-I



DEPARTMENT OF STATE

REFERENCE MANUAL
SECURITY REGULATIONS

FOR OFFICIAL USE ONLY

REFERENCE MANUAL
ON
SECURITY REGULATIONS

Prepared by Direction
of

Donald Russell

Assistant Secretary for Administration

REFERENCE MANUAL
ON
SECURITY REGULATIONS

This Reference Manual on Security Regulations has been provided as a handy reference copy of security regulations applicable to the Department and the Foreign Service. Keep this manual in your desk and refer to it frequently for guidance in respect to security practices and procedures to be employed. The contents of this reference manual are included also in the Administrative Manual as part of the Departmental Regulations.

All Departmental and Foreign Service personnel are required to read and understand the security regulations contained herein. A statement to this effect will be submitted to the Security Officer of the Department through the Security Officers of the various organizational units.

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

- I. GENERAL
- II. EXAMINATION AND CLASSIFICATION OF MATERIAL
- III. CATEGORIES OF CLASSIFIED MATERIAL
- IV. AUTHORITY TO CLASSIFY, APPROVE CLASSIFICATIONS AND DECLASSIFY OFFICIAL MATERIAL
- V. PREPARATION, REPRODUCTION AND MARKING CLASSIFIED MATERIAL
- VI. RESPONSIBILITY FOR SAFEGUARDING CLASSIFIED MATERIAL
- VII. DISSEMINATION AND DISTRIBUTION OF CLASSIFIED MATERIAL
- VIII. HANDLING AND TRANSMISSION OF CLASSIFIED MATERIAL
- IX. CUSTODY AND STORAGE OF CLASSIFIED MATERIAL
- X. OFFICE SECURITY
- XI. DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL
- XII. DEPARTMENTAL BUILDING SECURITY
- XIII. CRYPTOGRAPHIC SECURITY

201.1

201.1 SECURITY REGULATIONS OF THE DEPARTMENT OF STATE. (Effective 1-1-47)

I GENERAL.

A . The purpose of this regulation is to prescribe the security rules for classifying or grading, marking, reproducing, handling, transmitting, disseminating, storing, and destroying official material originating in or coming under control or jurisdiction of the Department of State and the Foreign Service.

B Official material originating in or coming under jurisdiction of the Department of State and the Foreign Service is of varying degrees of value to all nations, including any potential enemies of the United States, both internal and external, and, therefore, requires corresponding degrees of protection to prevent disclosure to unauthorized persons. Official material must be examined and, if protection is required, classified (or graded) in accordance with the degree of protection deemed necessary. The definitions and policies stated in this regulation are to insure the accurate and uniform classifying or grading and appropriate protection of official material.

C Definitions.

1 CLASSIFIED MATERIAL. Classified material refers to official material containing information to which a security classification has been assigned. As used herein, it also includes copies of official documents and any other official materials such as letters, instructions, memoranda, telegrams, airgrams, despatches, reports, notes, rough drafts, shorthand notes, carbons, and carbon copies which contain classified information.

2 CLASSIFYING OR GRADING. Classifying or grading includes rendering a decision relative to the degree of safeguarding required for a particular item of information and the act of stamping or otherwise marking, with an indication of one of the prescribed security classifications, the physical form in which the information appears.

3 CRYPTOGRAPHIC MATERIAL. Cryptographic material includes all documents and devices employed in changing plain-language messages into unintelligible form by means of codes and ciphers.

4 CRYPTOGRAPHIC SECURITY. A general term denoting the provision of technically sound cryptographic systems, their proper use, and their careful safeguarding.

5 CRYPTOGRAPHIC SYSTEM. Code and/or cipher and instructions therefor.

6 DECLASSIFYING. The act of removing entirely a previously imposed security classification, thus making the information involved *unclassified*.

7 DOCUMENTS. Any form of recorded information. The term *document* includes printed, mimeographed, typed, photostated, and written matter of all kinds; despatches, instructions, telegrams, memoranda, reports, minutes, airgrams, charts, maps, drawings, notes, or photostatic copies; photographs and photographic negatives; and all other similar matter.

201.1

I C (Continued)

8 DOWNGRADING. The act of lowering the assigned security classification of classified documents and material.

9 OFFICIAL MATERIAL. Information furnished to the Department and the Foreign Service in oral or documentary form in the conduct of official government business.

10 PARAPHRASING. A restatement of text in different phraseology without alteration of its meaning.

11 TELEGRAM. Any communication sent (or intended to be sent) by electrical means.

12 TRUE READING. The unparaphrased literal text of a telegram or airgram.

13 UPGRADING. The act of changing the assigned classification of official material upward.

14 STORAGE. Storage refers to the manner in which classified material is protected by physical or mechanical means or other security measures taken to protect classified material outside of working hours, or to the manner in which it is protected during working hours when not under personal supervision.

II EXAMINATION AND CLASSIFICATION OF MATERIAL.

A Official Material Will Be Examined. All originators of official material will make a determination as to the necessity of its being placed in one of the four security classification. If a security classification is required, the material will be graded and the physical form in which it appears will be marked TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED.

Note: The term UNCLASSIFIED will be used when it is essential to convey to a recipient of the material involved the fact that it has been examined with a view to imposing upon it an appropriate security classification and that a determination has been made that the material is *unclassified*. It is mandatory that all *unclassified* material moving through the diplomatic pouch, airgram, and telegram services of the Department be marked or stamped UNCLASSIFIED.

B Classifying or Grading.

1 Persons authorized to classify official material are outlined in paragraph IV.

2 Each document will be graded or classified according to its own content and not necessarily according to its relationship to another document except telegrams referring to previously classified telegrams (see paragraph XIII B). This also applies to extracts from classified documents, except certain telegrams which bear the notation "paraphrase before communicating *****" Extracts from such telegrams will be classified the same as the telegrams from which taken unless the extracts are paraphrased. If paraphrased, such extracts may be classified according to the nature of their contents.

C Only One Security Classification. Only one security classification will be assigned to a single document or device.

(1-1-47)

(TL 39)

ii (Continued)

D **File of Documents.** The classification of a file or group of physically connected documents will be that of the highest classified document contained therein. A letter of transmittal will be classified at least as high as any of its enclosures.

E **Overclassification.** Documents or material requiring classification under the provisions of these regulations will be assigned the least restrictive classification consistent with the proper safeguarding of the information or material concerned. *OVERCLASSIFICATION MUST BE AVOIDED* since it causes unnecessary delay and expense in the handling and transmission of documents, overburdens storage facilities, and depreciates the importance of classified information in the minds of handling personnel.

F **Automatic Downgrading or Declassifying.** Whenever practicable the classifying officer will place a notation on the document that upon the happening of a specified event or on a named date, the classification of the document will be reduced automatically to a stated lower classification or cancelled altogether without reference to the originating or higher authority. In the case of telegrams it will be necessary to include within the text any instructions relative to automatic downgrading or declassifying. Such instructions are in addition to the notation *Verbatim Text* required by the provision of paragraph V C 5a below. (See also paragraph IV B below).

G **Classification of Material From Other Government Agencies.** Matter obtained from the War and Navy Departments, other Government agencies, or foreign governments will be maintained by the Department and Foreign Service in the same or equivalent classification category as that in which it was placed by the originating agency.

iii CATEGORIES OF CLASSIFIED MATERIAL.

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 matters in time of peace will be limited to those which in and of themselves, if disclosed without authorization, would reasonably be expected to lead directly to a definite break in diplomatic relations or to a war or have other comparatively grave consequences.

1 **Very Little Material or Information Belongs in the TOP SECRET Category.**

2 The following are some examples of material or information which normally will be graded TOP SECRET:

a Information or material regarding or details of discussions or negotiations with foreign governments on questions of great delicacy, the premature disclosure of which would reasonably be expected to lead directly to a definite break in diplomatic relations or to a war.

b Informational or intelligence material containing indications of sources of intelligence where it is of paramount importance to the United States to protect the source in order to insure a continuance of the receipt of intelligence from the sources and where the unauthorized

201.1

III A 2 b (Continued)

disclosure of the sources would cause exceptionally grave damage to the United States through the loss of intelligence from such sources or would place individuals constituting the sources in extreme jeopardy of life or limb. *Very few* intelligence sources come within this category.

c Information or material concerning the existence or details of new devices or methods of warfare of extreme importance to national security. Such information normally will be classified TOP SECRET by the military or naval forces.

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.

1 The following are some examples of official material or information which normally will be graded SECRET:

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

b Important information or material obtained from or for transmission to high levels of the Government, the premature disclosure of which might endanger the success or effectiveness of a program or policy of *great importance* to the United States Government.

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

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

e Vital information on important defenses. Such information normally will be classified SECRET by the military or naval forces.

f High-grade cryptographic devices and related material.

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

1 *The Major Portion of Information Should be Classified no Higher Than CONFIDENTIAL.*

2 The following are some examples of official material or information which normally will be classified CONFIDENTIAL:

a Important intelligence reports.

III C 2 (Continued)

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

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

d Consultative inter-Departmental communications on questions of policy where disclosure might precipitate undesirable public controversy.

e Important information or material obtained from or for transmission to high levels, the unauthorized disclosure of which would greatly embarrass the Department or the source.

f Certain cryptographic devices and related material.

D **Restricted.** Information or material which does not fall within higher categories but which should not be communicated outside the Government without adequate clearance will be classified RESTRICTED.

1 The following are some examples of official material or information which normally will be graded RESTRICTED:

a Certain economic, industrial, or political information which should not be released or communicated to the press or otherwise published and made available to the public.

b Interpretations representing official Department views and based on official or public reactions to general international or economic questions.

c Administrative or instructional communications and documents requiring the protection of a security classification, which are intended strictly for official use within the Department or the Foreign Service.

d Reports on certain internal affairs of the United States and of foreign countries which should not become public knowledge.

E **Unclassified.** Material not marked with one of the above security classifications will be understood to be UNCLASSIFIED.

1 Material not falling into one of the above classifications but which is to be forwarded by telegram, airgram, or diplomatic pouch facilities will be marked UNCLASSIFIED. This marking is not otherwise obligatory and is used only on material transmitted by one of the above mentioned facilities to assure that it has been reviewed and appropriately classified or graded.

IV AUTHORITY TO CLASSIFY, APPROVE CLASSIFICATIONS AND DECLASSIFY OFFICIAL MATERIAL.

A **Classifying or Grading.** The originator of a document will be responsible for imposing a security classification on it, as required, appropriate to its contents. The security classification imposed will be subject to the following procedures for review and approval:

200.1

HW A (Continued)

1 TOP SECRET.

a The imposition of the Classification TOP SECRET on material will require, in each instance, the personal approval of the Director of an Office, or higher authority, their respective deputies, or officers specifically designated in writing by them to act in their absence or for emergency cases. In the Foreign Service the use of the TOP SECRET classification will require, in each instance, the personal approval of the Officer in Charge, the next ranking officer or, in the case of Embassy Staffs only, the Chiefs of major subdivisions of such staffs.

b The official record file copy of TOP SECRET material, in addition to being stamped or marked TOP SECRET, will be marked with the date of classifying and the words *classification approved* adjacent to the classification mark, and will be initialed by an authorized approving officer, as indicated above, in a space provided following the words *classification approved*.

2 SECRET.

a The imposition of the SECRET classification will require, in each instance, the personal approval of the Chiefs of Divisions, or higher authority, their respective deputies, or an officer specifically designated in writing by them to act in their absence or for emergency cases. In the Foreign Service, the use of the SECRET classification will require, in each instance, the personal approval of the Officer in Charge, the next ranking officer or, in the case of Embassy Staffs only, the Chiefs of major subdivisions of such staffs.

b The official record file copy of SECRET material, in addition to being stamped or marked SECRET, will be marked with the date of classifying and the words *classification approved* adjacent to the classification mark and will be initialed by an authorized approving officer, as indicated above, in a space provided following the words *classification approved*.

3 CONFIDENTIAL AND RESTRICTED. Any originator of official material may cause such material to be classified CONFIDENTIAL or RESTRICTED as warranted by the contents.

4 The Security Officer of the Department will review, from time to time, the use of all security classifications throughout the Department and the Foreign Service in order to insure uniform and proper usage. For this purpose, he will collaborate closely with Administrative or Executive Officers of Divisions or Offices and designated Officers in the offices of Assistant Secretaries and higher levels.

B Downgrading and Cancelling Classifications.

1 It is the obligation of all officers to keep classified matter of current interest or continuing value constantly under review and to downgrade it as soon as conditions permit.

2 When it is desired to downgrade documents of the same type which accumulate in bulk, authority to downgrade or declassify in bulk will be obtained from the Security Officer.

201.1

IV B (Continued)

3 Material which has been classified solely to accord with conditions imposed by a foreign nation may be downgraded or declassified with the consent of the nation concerned or by approval of the Secretary or Under Secretary.

4 MATERIAL FROM OTHER DEPARTMENTS OR AGENCIES. Material originated in other Departments or Agencies cannot be reduced in classification except with consent of that Department or Agency. If it is desired to retain such material and to reduce it in classification, the Division should make a list of the material and send it to that Department or Agency requesting that the material be reduced in classification. Material which originated in agencies which are no longer in existence should be referred to the Security Officer, Department of State, who will take appropriate action.

5 The officer imposing the original classification, (not necessarily the approving officer), or higher authority, may cancel or change the classification of a document by writing or stamping over or adjacent to the classification mark at the top of the first page, "Classification changed to _____, by authority of (name of officer making the change, office symbol, and the date thereof)." An exception to the above is made in the case of telegrams containing the notation "paraphrase before communicating*****".

6 (a) The officer on cancelling or changing the classification of material will notify the custodian of the official Department record copy. When considered necessary and feasible, the officer effecting the cancellation or change in classification will notify all offices or personnel concerned, by memorandum, of the cancellation or change in classification of the material. Such memoranda of notification may be informal in nature, e.g. in hectographed form.

(b) In the case of telegrams marked "Paraphrase Before Communicating*****", no change in classification will be made unless the text has been carefully paraphrased and the serial number of the original telegram and any to which reference has been made have been deleted, except that messages classified TOP SECRET may be downgraded to SECRET when their content warrants.

(c) The true reading of a telegram marked "Paraphrase Before Communicating*****" and classified TOP SECRET or SECRET will not be reduced to a classification below CONFIDENTIAL earlier than 5 years following the date of the telegram. The true reading of classified telegrams may be declassified if the telegrams are over 10 years old and if the declassification action is warranted by the contents of the telegrams.

7 The declassification and downgrading procedure of the Department is outlined in detail in Departmental Regulation 201.3.

8 A Declassification Committee, consisting of the Security Officer of the Department and one representative each from the Office of the geographic area concerned with the material being considered for declassification, Office of Foreign Service (OFS), and Office of Intelligence Coordination and Liaison (OOL) will act as the final arbiter in cases where there is a lack of agreement on the downgrading or declassification of any item of information.

201.1

V PREPARATION, REPRODUCTION AND MARKING CLASSIFIED MATERIAL.

A Preparation and Reproduction of Classified Material. Classified material will be prepared with a minimum number of copies as the risk that classified material may fall into unauthorized hands increases in proportion to the number of copies in existence.

1 PRINTING OR REPRODUCTION. The Officers directing the preparation, printing, or reproduction of classified material will cause strict supervision to be exercised over the disposition of the notes, manuscripts, type, plates, stencils, negatives, and wastage incident thereto, in a manner which will properly safeguard the information being reproduced.

2 NOTATION OF REPRODUCTION. The copy of TOP SECRET, SECRET, or CONFIDENTIAL material, from which reproduction is made will contain or have attached thereto a notation relative to the authority for reproducing the material and the number of copies made.

3 DISTRIBUTION OF REPRODUCED MATERIAL. Except for Divisions of the Department authorized to make regular distribution of material, no distribution of material (classified higher than RESTRICTED) reproduced will be made outside of the reproducing Division unless specifically authorized by a responsible officer of the originating Division, or by the Chief or his Deputy of the Division having jurisdictional control over it if it originated in a Foreign Service Post.

4 MATERIAL FROM OTHER DEPARTMENTS.

a SECRET or CONFIDENTIAL material originating in another Department or Agency of the Federal Government will not be copied or otherwise reproduced in the Department or Foreign Service without approval of the originator or other individual in the Department or Agency having authority to approve such reproduction, except that Chiefs of Divisions or higher authority may authorize reproduction of such material after consideration of the necessity for reproduction in each instance.

b Distribution outside the reproducing Division of reproduced material originating in another Department or Agency must be specifically authorized in each instance by a responsible officer of the originating agency.

5 REPRODUCTION OF TOP SECRET MATERIAL.

a TOP SECRET material originating in the Department will not be copied or otherwise reproduced in any organizational unit, other than the originating office, without authorization in writing of the Director, or his Deputy, of the Office in which the material originated, or higher authority. At a Foreign Service Post, reproduction of such material must be authorized in writing by the Officer in Charge or the next ranking officer.

b TOP SECRET material originating in a Foreign Service Post will be copied or otherwise reproduced in the Department, if reproduction is essential, only in the Division receiving the material for action, or if the material is of purely informational character, in the Division of the Department receiving the material as a matter of primary interest, except

201.1

V A 5. b (Continued)

that the Chief of the Division receiving such material for action or as a matter of primary interest may, in writing, authorize another Division to reproduce such material provided strict control is maintained over the reproduction process and all copies are strictly accounted for.

c TOP SECRET material originating in another Department or Agency of the Federal Government will not be copied or otherwise reproduced in the Department or Foreign Service without specific approval in each instance of the originator or other responsible individual in the Department or Agency concerned having authority to approve reproduction.

6 COPIES OF TELEGRAMS. The Division of Communications and Records (DC) will reproduce all copies of all telegrams and airgrams required for authorized distribution.

B Marking of Classified Material. When an officer specifies that official material is to have a security classification, the stenographer will indicate on the material the classification and any additional markings required in accordance with the following rules:

1 FORMAL LETTER COMMUNICATIONS. Conspicuously stamp or type the classification in the *upper left corner* and *center bottom* of the first sheet and at the *center top* and *bottom* of each succeeding sheet. When the form permits and the number of copies is small, the classification will be indicated by means of a rubber stamp and colored ink; otherwise, it will be typed in underlined capital letters.

a Office memoranda and other informal communications will have the classification stamped or typed in the *top center* and *bottom center* of each page.

2 TELEGRAMS. The classification assigned a telegram will be conspicuously marked or stamped at the *top* and *bottom* of *each sheet* of the telegram form. Paraphrased copies of classified telegrams also will be stamped or marked with the appropriate classification at the *top* and *bottom* of *each page*.

3 BOOKS AND PAMPHLETS. The classification of books and pamphlets, the pages of which are permanently and securely fastened together, will be shown on the cover, title page, first page, back page, and back cover.

4 MIMEOGRAPHED OR HECTOGRAPHED, MULTILITH AND OZALID REPORTS, DESPATCHES, ETC. Reports, despatches, etc., reproduced in mimeograph or hectograph, multilith and ozalid form and bound with staples will be stamped or marked with the classification on the *center top* and *bottom* of *each page*.

5 CLASSIFIED DRAWINGS OR TRACINGS. Classified drawings or tracings will carry a legend of the proper classification in such a position that it will be reproduced on all copies made therefrom. Whenever practicable, classified photographic negatives will be marked in the same manner. Classified motion picture films will be kept in containers which bear the classification mark to which the contents are entitled, and in addition will state in the title the classification thereof. Classified sound recordings will contain

201.1

V B 5 (Continued)

an opening and closing statement indicating the classification of the recording and will be marked with the appropriate classification in the best manner practicable. If marking of the recording is not practicable, its container will be marked.

6 CONTRACTS FOR THE MANUFACTURE OF CLASSIFIED MATERIAL. Contracts for the manufacture of classified material will be plainly and conspicuously marked or stamped with the proper classification on the *center top* and *bottom of each page*.

7 CLASSIFIED MAPS AND PHOTOMAPS. Classified maps and photomaps will be appropriately marked under the scale and on the *top* and *bottom of each sheet*.

C Additional Marking of Classified Documents

1 DOCUMENTS ISSUED TO AUTHORIZED PRIVATE INDIVIDUALS. Documents containing classified information authorized to be furnished to persons not employed by the Federal Government will, in addition to being marked with the security classification, bear the following notation:

This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, or information of vital interest to the Federal Government and is transmitted for official use only.

2 U. S. OFFICIALS ONLY. Documents so marked will be shown to or viewed by officials of the United States Government only. *Note:* Classified telegrams will not be shown to or viewed by other than U. S. officials except under the conditions specified in paragraph XIII D 2.

3 SPECIAL MARKING OF TOP SECRET AND SECRET DOCUMENTS. All TOP SECRET and SECRET documents will show on the record copy the authority for the classification, the initials of the officer approving the classification and the date affixed. (See Paragraphs IV, A1 and 2.)

4 MARKING FOR LOOSE FILE. The top document or covering paper of a group or file of associated papers will contain an indication of the classification of the highest graded material contained therein. In assembling a file, if any of the under papers have a classification higher than that of the topmost document, a sheet of paper or transmittal slip conspicuously stamped or marked with the classification of the highest classified material contained therein will be used to cover the whole file.

5 SPECIAL MARKINGS FOR TELEGRAMS.

a The words *VERBATIM TEXT* will be placed at the top of the first page of each outgoing telegram containing a verbatim quotation from a note, an agreement, or other document, which has been or is intended to be shown or communicated to officials of foreign governments, the press or similar entities outside the U. S. Government. The notation, *VERBATIM TEXT* will also be used whenever the drafting officer knows that the information in the telegram has been discussed with or is liable to be released in the near future to persons outside the U. S. Government.

201.1

V C 5 (Continued)

b For convenience or economy it may be desirable to transmit in airgram form the text or a portion of the text of a telegram which has been sent or received in encrypted form. When such airgrams are identified with the telegram quoted, they will bear the following notation at the top of the first page:

This airgram contains information taken from an encrypted telegram and must be handled as prescribed for the true reading of such telegrams.

c All true readings or paraphrased versions of classified telegrams communicated to persons outside the Department or the Foreign Service will bear the following notation:

Reproduction of this message in any form is not authorized.

VI RESPONSIBILITY FOR SAFEGUARDING CLASSIFIED MATERIAL.

A The responsibility for the maintenance of the security of classified information rests upon each person having knowledge thereof, *no matter how obtained.*

B Public or private discussion of classified information with or in the presence or hearing of any person not authorized to have knowledge thereof is strictly forbidden. This rule is aimed especially at persons inclined to engage in discussions of office affairs with their families or friends outside of the office; it also applies to careless talk in the office in the presence of visitors or workmen, talk in public places, and talk over the telephone involving information classified higher than Restricted.

C **Approval for Public Dissemination.** The inclusion of classified information or material under jurisdiction of the Department or the Foreign Service in any public lecture or course of instruction given or article or book published by an employee of the Department of State or the Foreign Service is strictly prohibited unless specifically authorized by the Secretary of State, one of the Under Secretaries or by the Committee on Unofficial Publication (See Departmental Regulation 183.3, effective 1-1-46.)

1 The above regulation does not preclude the appearance of employees of the Department or Foreign Service before audiences in government operated schools or in official training or indoctrination programs after appropriate clearance has been given of the classified information or material involved.

2 The regulation stated in paragraph VI C above is in addition to and is not to be construed as being in conflict with the provisions of Departmental Regulation 234.3, "Information Issued to the Public" (effective 1-1-46); Departmental Regulation 234-c, "Public Appearances by Department Officers" (effective 2-13-46); and Departmental Regulation 393-b, "Limitation on Activities of Officers of the Department of State and of the Foreign Service in Connection with Programs and Activities of Private Organizations" (effective 6-21-45).

201.1

VI (Continued)

D **Unauthorized Publication or Dissemination.** The unauthorized publication or other unauthorized dissemination of classified material of the Department or Foreign Service is prohibited by law. Section 135, title 22 of the United States Code provides as follows:

Whoever, by virtue of his employment by the United States, shall obtain from another or shall have custody of or access to, or shall have had custody of or access to, any official diplomatic code or any matter prepared in any such code, and shall willfully, without authorization or competent authority, publish or furnish to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

Note: Most classified material in the Department or Foreign Service has been or will have been transmitted in coded form at some time.

E Although material or information having a security classification may not be communicated to the press, the classification of such material or information may be cancelled in accordance with paragraph IV B and Departmental Regulation 201.3, and the information then released to the press through authorized press relations channels, or, in the case of material which must be released for publication abroad, by authority of the Chief of Mission or higher authority.

F **Testimony Before Congress.**

1 When an employee of the Department of State appears before a committee of the Congress and is called upon to give testimony which he knows to be CONFIDENTIAL or RESTRICTED, he will respectfully request that his statements be taken in executive session only and not appear in the record of hearings, the Congressional Record, or other documents open to public inspection.

2 When called upon to give testimony which he knows to be TOP SECRET or SECRET, unless he has previously been authorized by the Secretary of State to give such testimony, he will respectfully state that he is not authorized to disclose the information desired, and will inform the appropriate Member of Congress that a written request for the specific information should be transmitted to the Secretary of State. Testimony of a TOP SECRET or SECRET nature, when authorized by the Secretary of State, will be given only in executive session under the conditions cited in paragraph 1 above.

G **Instruction of Newly Assigned Personnel.** Upon assignment of new officers or clerical personnel who have any part in the preparation, handling, or transmission of classified material, it is the responsibility of the Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities to ensure that such newly assigned personnel receive adequate instruction in the security regulations and procedures of the Department and Foreign Service.

H **Separation of Personnel From Department or Foreign Service.** Personnel leaving the Department or Foreign Service are not authorized, upon separation therefrom, to communicate to anyone information of a classified nature obtained while in the employ of the Department or Foreign Service. Prior to obtaining

VI H (Continued)

clearance for final salary payment, each employee being separated from the Department will turn in all classified material, identification passes, and keys issued to him while in the employ of the Department. A statement will be obtained from each employee prior to his separation from the Department that none of such material or equipment remains in his possession. Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities will be responsible for instructing personnel leaving the Department or Foreign Service in respect to the above.

VII DISSEMINATION AND DISTRIBUTION OF CLASSIFIED MATERIAL.

A Knowledge or Possession of Classified Matter. No person is entitled solely by virtue of his grade or position to knowledge or possession of classified material. Such material will be entrusted only to those individuals whose official duties require such knowledge or possession.

B Distribution of Classified Information Within the Department and Foreign Service. Distribution of classified material to persons within the Department of State and the Foreign Service will be made on the basis of their functional requirements for such information. Requirements for such information will be determined by the Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service Posts, or by higher authority on the basis of the relationship of persons concerned to a specific undertaking or to general background requirements. The intelligent enforcement of the above-mentioned rule is dependent upon the understanding and collaboration of all responsible officers. In order to facilitate the attainment of the desired objectives, the following procedures are established:

1 Within the Department, the Chief of the Division of Communications and Records (DC) will be responsible, after having been notified of the functional requirements of the various offices and after consultation with the appropriate Chiefs of Divisions, Directors of Offices and higher authorities, for assuring that incoming telegrams, airgrams, despatches, reports, and other materials are properly distributed to organizational units on the basis of organizational functions as defined by Departmental Regulations. Similar responsibilities for the distribution of classified material will be discharged by appropriate officers in the various field offices of the Foreign Service.

2 The Administrative or Executive Officers of the originating or action Division, Office, or Foreign Service establishment, after consultation with their respective chiefs and after consideration of requests from other offices, will be responsible for assuring that there is proper distribution, both within their own offices and to other offices, of all material which originates with their organizations or coming under their jurisdiction for action in the Department or the Foreign Service, and in departmental committees and inter-Departmental committees on which the Department of State is represented. Only established channels of distribution will be utilized.

3 Any disagreement as to the right of an office or person of the Department to receive certain classified information will be referred, in the first instance, to the Directors of Offices or Staff Officers concerned, for direct consideration. If a satisfactory arrangement is not achieved through

201.1

VII B 3 (Continued)

such consultations, the disagreement will be referred through proper channels to the officer of the lowest level having common jurisdiction over both disputants or to the Assistant Secretary for Administration or his Deputy, if it is at the staff level. Disagreements in a single establishment of the Foreign Service abroad will be resolved by the Officer in Charge directly concerned.

C Special Rules for Dissemination of Top Secret Material.

1 TOP SECRET material and information will receive the absolute minimum dissemination within the Department and the Foreign Service. It is exclusively for the official use of officers who deal directly with the subject matter and of other persons who have been specifically designated by those officers to work with such material and information. TOP SECRET material and information will be disseminated outside the Department and the Foreign Service only to officers of Federal Departments and Agencies who are known to be qualified to receive it.

2 Each individual of the Department or Foreign Service whose duties require that he work on or have access to TOP SECRET material will first be certified by the Security Officer of the Department for access to such material. A list of personnel in the Department for which certification to handle TOP SECRET material is desired will be furnished to the Security Officer of the Department by Administrative or Executive Officers of Divisions, Offices and higher levels. A list of personnel in each Foreign Service establishment authorized by the Officer in Charge to handle TOP SECRET material will be maintained by the Security Officer of the Mission and a copy thereof furnished to the Security Officer of the Department for certification.

3 A record will be made on each TOP SECRET document of all persons who have had access to it or have read it.

D Dissemination of Classified Material Outside the Department.

1 Copies or paraphrases of classified material which have originated in the Department or Foreign Service will not be sent to other Federal departments or agencies, or to designated individuals therein, except by an officially signed or initialed transmitting communication or through the official liaison Divisions of the Department whose specific duty it is to make formal distribution and keep records of the material distributed.

2 Classified material originating in another Department or Agency and furnished to the Department of State will not be communicated to a third Department or Agency without the consent of the originating Agency.

3 All requests from private individuals, firms, corporations, or state or municipal agencies for classified information or material of the Department must be addressed to the Department in written form before they will be acted upon. Such requests will be forwarded to the Security Officer of the Department for a review of the security considerations involved when TOP SECRET, SECRET, or CONFIDENTIAL material or information is involved, or when there is any doubt as to the qualification of the person or agency to receive

201.1

VII D 3 (Continued)

RESTRICTED material or information requested or when the need therefor is not clearly justified. Releases of material or information classified higher than RESTRICTED will be made *only for the most compelling reasons*.

a Material or information classified RESTRICTED may be made available to private individuals, firms, corporations, or state or municipal agencies provided *all* of the following conditions apply:

(1) A request in writing has been submitted by the requesting agency for each document or item of information desired. Such requests must state the reason the material is desired and the intended use thereof.

(2) Release of the material or information is clearly advantageous to the Department and is in the national interest.

(3) Department of State or U. S. Government policy on release to the public will not be violated by release of the requested material or information.

b Each request for RESTRICTED material or information of the Department will be submitted to the Division of Public Liaison (PL) who will forward it to the Chief of the originating or action Division and, when appropriate, to the Security Officer of the Department for the purpose of determining whether the material or information involved can be declassified and released or whether release can be made in *classified* form.

c Each request for material or information classified *higher* than RESTRICTED will be submitted to the Division of Public Liaison (PL) who will forward it to the Chief of the originating or action Division and to the Security Officer of the Department *in turn* for the purpose of determining whether the material requested can be declassified and released, or whether it can be released in *classified* form. Release of such material *will not be made* without the concurrence of *both* the Chief of the originating Division and the Security Officer of the Department.

d Each request for use of Departmental records by persons who are not officials of the United States Government will be referred to the Division of Historical Policy Research (RE) who will act on such requests in accordance with the principles outlined in sub-paragraphs a, b and c above and in accordance with Departmental Regulation 420.1 and other pertinent regulations.

4 When classified material is disseminated under the provisions of these regulations to persons not employed by the Federal Government, they will be informed in the first instance of the proper safeguards required for the handling and storage of the category of material furnished, so that adequate protection may be provided therefor. Official material containing classified information furnished persons not employed by the Federal Government will, in addition to being marked with one of the security classifications, bear the following notation:

This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, or information of vital interest to the Federal Government and is transmitted for official use only.

201.1

VIII HANDLING AND TRANSMISSION OF CLASSIFIED MATERIAL.

A Use of the Telephone.

1 Information classified *higher* than RESTRICTED will not be transmitted by telephone within the Department or to outside agencies. This rule applies also to establishments of the Foreign Service abroad.

2 It is permissible to *make reference* by telephone to material classified higher than RESTRICTED if such references do not, in the course of conversation, reveal the substance of those portions of material under discussion which are classified higher than RESTRICTED. References to file numbers, dates, and subject (provided the subject itself is not classified higher than RESTRICTED) may be made over the telephone, but great care must be exercised not to reveal substantive matter classified higher than RESTRICTED.

B Transmission of Classified Material.

1 TOP SECRET.

a TOP SECRET material will be handled and transmitted in accordance with the rules given in paragraph b below. The following precautions will be strictly observed:

(1) The transmission of TOP SECRET information will be effected by direct contact wherever practicable.

(2) It is mandatory that transmission and custody of TOP SECRET material be covered by a receipt system.

(3) Under no circumstances will TOP SECRET material be transmitted by registered mail.

(4) Under no circumstances will TOP SECRET telegrams be transmitted by electrical means in the clear.

b
Post.

Transmission within the Department or within a Foreign Service

(1) TOP SECRET material will be transmitted between organizational units of the Department or within a Foreign Service Post by hand of officer or other trustworthy personnel who has worked with the material. Within the Department, transmission of TOP SECRET material via the Security Messenger Service also is authorized.

(2) Material forwarded by hand of officer or other trustworthy personnel who has worked with the material will be enclosed in at least one envelop or otherwise effectively covered from view.

(3) Material forwarded via the Department's Security Messenger Service will be enclosed in double sealed envelopes. The *inner envelope* will be clearly and plainly stamped or marked TOP SECRET and addressed to the specific officer for whom it is destined by name, office symbol, room number, and building. The *outer envelope* will be similarly addressed and clearly marked VIA SECURITY MESSENGER SERVICE. No security classification will be marked on the outer envelope.

(1-1-47)

(TL 39)

201.1

VIII B 1 b (Continued)

(4) A receipt (Form DS-406 or other suitable receipt form) will be executed covering the transfer of TOP SECRET material, whether transmitted by hand of officer or clerical personnel or by the Security Messenger Service. If transmitted by the Security Messenger Service, the Receipt Form DS-406 will be attached to the *outer* envelop. *Note:* The regular messenger service of the Department is *not* approved for the transmission of TOP SECRET material.

(5) Transmission of TOP SECRET material within the Department by any means other than those described in paragraph b(1) above is not authorized unless specifically approved by the Departmental Security Officer. Transmission of TOP SECRET material within a Foreign Service Post by any means other than those described in paragraph b(1) above is not authorized unless specifically approved by the Security Officer of the Post concerned.

(6) Typewritten material in documents will be protected from direct contact with the inner cover by a cover sheet or, if the documents are folded, by folding inward.

Transmission to a Foreign Service Post.

(1) If review by the Division of Coordination and Review (CR) is necessary prior to dispatch, each separate TOP SECRET letter, memoranda, note, instruction, or other TOP SECRET material will have attached a *single unsealed* opaque envelope addressed to the officer in charge of the Foreign Service Post, or to an individual by name, and marked *TOP SECRET - TO BE OPENED ONLY BY THE OFFICER IN CHARGE* (or the name of an individual authorized to handle TOP SECRET instead of to *THE OFFICER IN CHARGE*). The correspondence will be transmitted to the Chief of the Division of Coordination and Review (CR) in a manner prescribed for transmission of TOP SECRET material within the Department. (See paragraph VIII B 1 b.) A receipt will be executed covering delivery of each piece of TOP SECRET material to the Division of Coordination and Review (CR).

(2) After completion of the review process the Division of Coordination and Review (CR) will transmit, by an authorized means, each TOP SECRET communication involved to the proper section of the Division of Communications and Records (DC) for forwarding by Diplomatic Fouch.

(3) If review by the Division of Coordination and Review (CR) is *not* necessary, each separate TOP SECRET document will be enclosed in a *single* opaque envelope addressed to the officer in charge of a Foreign Service Post, or to an individual by name, and marked *TOP SECRET - TO BE OPENED ONLY BY THE OFFICER IN CHARGE* (or the name of an individual authorized to handle TOP SECRET instead of *TO THE OFFICER IN CHARGE*). The envelope will be *sealed* and then transmitted to the Facilities Branch, Division

201.1

VIII B 1 c(3) (Continued)

of Communications and Records (DC) in a manner prescribed for transmission of TOP SECRET material within the Department. (See paragraph VIII B 1 b.) A receipt will be executed covering delivery of TOP SECRET material to the Facilities Branch, Division of Communications and Records (DC).

(4) TOP SECRET documentary material will be transmitted to a Foreign Service Post in the custody at all time of a Diplomatic Courier.

d
Post).

Transmission Outside the Department (Not to a Foreign Service

(1) TOP SECRET material to be transmitted to another Government Department or Agency will be enclosed in two sealed envelopes and transmitted by hand of officer or other trustworthy personnel who has worked with the TOP SECRET material involved, or will be transmitted via the Department's Security Messenger Service, by the courier system of other Departments or Agencies concerned (if such means are approved by the Departmental Security Officer) or by other means specifically approved by the Departmental Security Officer.

(2) The inner envelope will be addressed to an individual by name, title and full address and will be marked or stamped *TOP SECRET*. If transmitted by an approved messenger or courier system, other than the Department's Security Messenger Service, a receipt will be attached to the inner envelope to be signed by the addressee and returned to the originator. If transmitted by the Department's Security Messenger Service, the receipt form will be attached to the outer envelope.

(3) The outer envelope will be addressed to the individual showing his name, title and full address. *The outer envelope will not bear a security classification marking.*

(4) Correspondence sent through the Division of Coordination and Review (CR) will have attached the correct number of properly addressed envelopes, the inner one marked with the security classification.

(5) The receipt attached to an envelope, whether inner or outer, will be signed by the individual to whom the envelope is addressed, or by a responsible liaison officer, a TOP SECRET control officer, or other person known to be specifically designated to receive such material for the Department or Agency.

Receipt of TOP SECRET Material.

(1) Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service Posts, and higher authorities will appoint certain officers in their offices to be known as TOP SECRET Control Officers, with such assistants as necessary, who will

201.1

VIII B 1 e (1) (Continued)

receive and maintain a register of all TOP SECRET material coming to their respective organizations, and who will be responsible for exercising control over such material while it is in their office.

(2) TOP SECRET Control Officers will open and deliver TOP SECRET correspondence to such individuals as must see and work on the correspondence. Persons who work on TOP SECRET material will be kept to a minimum and will be individually warned against disclosing such matters to personnel whose duties do not require it. In addition, prior to permitting personnel to have access to TOP SECRET material, they will be certified by the Security Officer of the Department.

2 SECRET.

a Transmission within the Department or within a Foreign Service Post.

(1) Between buildings and between Divisions of different Offices located in the same building, SECRET material will be transmitted by hand of officer or other responsible personnel, or through the regular Messenger System of the Department. Transfer of SECRET material in such cases will be covered by receipt. If transmitted via the regular Messenger Service of the Department, Receipt Form DS-406 will be used.

(2) Between Divisions of the same Office located in the same building, SECRET material will be transmitted by hand of officer or other responsible personnel or by regular messenger. Transfer of SECRET material in such cases need not be covered by a receipt. Control of such material will be maintained by registering it in and out of the offices involved in the transfer of material.

(3) SECRET material forwarded through the Department's regular Messenger System or carried by hand of officer or other responsible personnel will be enclosed in a single sealed envelop. For this purpose, Receipt Form DS-406 will be used wherever practicable. The security classification will not be marked on the envelope in such cases.

(4) Transmission of SECRET material within the territorial jurisdiction of a Foreign Service Post will be accomplished by diplomatic courier, either an officer of a Foreign Service Post or a regularly assigned courier of the Diplomatic Pouch and Mail Service, an officer of the Armed Services or through the courier facilities of the Armed Services. Within and between buildings of a Foreign Service Post a messenger service utilizing U. S. citizens only and approved by the Security Officer of the Post may be used. Transfers by such means will be covered by receipts.

201.1

VIII B 2 a (Continued)

(5) Telegrams, airgrams, despatches, and other similar SECRET material which are *regularly* distributed from a central distribution point, where a record of distribution is kept, will be covered by a receipt, one receipt covering the entire contents of a single envelope. Office Message Centers and other subdistribution points, will obtain receipts for SECRET material distributed to other than their own Divisions located in the same building in which the Office Message Center is located.

(6) Transfers within the Department of SECRET material received from other Departments or Agencies of the Government will be covered by receipt in each instance of a transfer within the Department of State.

(7) Typewritten material in documents will be protected from direct contact with the inner cover by a cover sheet or, if the documents are folded, by folding inward.

(8) The envelope enclosing SECRET material will be opaque and will be addressed by name, office symbol, room number and building. No classification stamp or mark will be used on the envelope to indicate its SECRET contents.

(9) Within the Department, receipts attached to envelopes containing SECRET material will be signed by the addressees and returned through the regular Messenger System to the senders.

Transmission to a Foreign Service Post.

(1) If review by the Division of Coordination and Review (CR) is necessary prior to dispatch SECRET letters, memoranda, notes, instructions, or other SECRET material will have attached single *unsealed* opaque envelopes addressed to the officer in charge of the Foreign Service Post, or to an individual by name, and will be marked *SECRET*. Such material will be transmitted to the Division of Coordination and Review (CR) in a manner prescribed for transmission of SECRET material within the Department. Receipts will be executed covering delivery of the SECRET material to the Division of Coordination and Review (CR).

(2) After completion of the review process, the Division of Coordination and Review (CR) will transmit, by an authorized means, the SECRET communications involved to the proper section of the Division of Communications and Records (DC) for forwarding by Diplomatic Pouch.

(3) If not cleared through the Division of Coordination and Review (CR), SECRET material will be enclosed in a single *sealed* envelop, completely addressed, and stamped *SECRET*, and the

201.1

VIII B 2 b (3) (Continued)

envelop will be transmitted by an approved means to the Facilities Branch of the Division of Communications and Records (DC) for forwarding via Diplomatic Fouch facilities. Receipts will be executed covering delivery of such SECRET material to the Facilities Branch of DC.

(4) SECRET material will be transmitted to a Foreign Service Post under custody at all times of a Courier designated by the Diplomatic Courier Service.

c
Post).

Transmission Outside of the Department (not to a Foreign Service

(1) SECRET material, other than cryptographic material (see paragraph XIII F 3) to be transmitted outside the Department, except to Foreign Service Posts, will be enclosed in two sealed envelopes and transmitted by hand of officer or other responsible personnel, by the messenger system of the Department or Agency to which the material is addressed (if such transmission means is approved by the Departmental Security Officer) or by United States Registered Mail with return receipt requested.

(2) Both envelopes will be properly and completely addressed, and the inner one marked SECRET. The outer envelope will not be stamped or marked with the security classification.

(3) A receipt will be attached to the inner envelope for signature of the addressee and return to the sender.

3 CONFIDENTIAL. CONFIDENTIAL material will be prepared and transmitted in accordance with the following rules:

a
Post.

Transmission within the Department or within a Foreign Service

(1) CONFIDENTIAL material will be prepared and transmitted within the Department or within a Foreign Service Post by hand of officer, responsible clerical personnel, or through the regular messenger system, if such means is approved for handling CONFIDENTIAL material by the appropriate Security Officer (the Departmental Security Officer in the case of material transmitted within the Department or the Security Officer of the Foreign Service Post concerned in the case of material transmitted within a Foreign Service Post).

(2) The regular messenger service of the Department is authorized for transmission of CONFIDENTIAL material.

(3) Transmission of CONFIDENTIAL material need not be covered by a receipt unless deemed necessary by the sender in cases of unusual importance.

201.1

VIII B 3 a (Continued)

(4) CONFIDENTIAL material will be prepared for transmission in double sealed envelopes except when transmitted via hand of officer, responsible clerical personnel, or the regular Messenger System of the Department, in which case a single envelop will be used. When double envelopes are used, both will be addressed with the name, room number and building of the addressee and the inner envelop will be stamped or marked CONFIDENTIAL. The outer envelop will not be marked with the security classification. When transmitted via the Department's regular Messenger System the single envelop used will be opaque and will contain the name, room number, and building of the addressee. No security classification will be indicated thereon.

b Transmission to a Foreign Service Post.

(1) CONFIDENTIAL material will be transmitted to Foreign Service Posts by Diplomatic Fouch facilities.

(2) CONFIDENTIAL material for transmission via Diplomatic Fouch facilities will be forwarded to the Facilities Branch, Division of Communications and Records (DC) by a means authorized for transmission of CONFIDENTIAL material within the Department or, if such material must be reviewed by the Division of Coordination and Review (CR), it will be transmitted to CR via an authorized means, and CR will accomplish transmission to the Facilities Branch of the Division of Communications and Records (DC).

(3) If the material is reviewed by the Division of Coordination and Review (CR), a completely addressed, unsealed envelop, marked or stamped CONFIDENTIAL will be attached to the file.

(4) If not reviewed by the Division of Coordination and Review (CR), the material will be enclosed in a sealed envelope, bearing the complete address of the individual in the Foreign Service Post for whom the communication is destined, and will be stamped or marked CONFIDENTIAL. Transmission to the Facilities Branch, Division of Communications and Records (DC) will be accomplished in a manner approved for transmission of CONFIDENTIAL material within the Department.

c Transmission Outside of the Department (Not to a Foreign Service Post).

(1) CONFIDENTIAL material to be transmitted outside of the Department will be enclosed in double sealed envelopes and transmitted by hand of officer or other responsible personnel, by the regular Messenger System of the Department or Agency to which the material is addressed, (if approved by the Departmental Security Officer), or by United States Registered Mail with return receipt requested.

(2) Both the inner and outer envelopes will be completely addressed. The inner envelope will be stamped or marked CONFIDENTIAL. The outer envelope will not be marked with the security classification.

VIII B 3 c (Continued)

(3) Transmission of CONFIDENTIAL material need not be covered by a receipt unless the sender considers the material involved of unusual importance.

4 RESTRICTED. RESTRICTED material will be prepared for transmission in a single opaque envelope bearing no security classification.

a Within the Department. RESTRICTED material will be transmitted within the Department through the regular Messenger System of the Department or by hand of responsible person.

b To a Foreign Service Post. RESTRICTED material will be transmitted by Diplomatic pouch facilities. RESTRICTED material will be sent to the Facilities Branch, Division of Communications and Records (DC) in a manner prescribed for transmission of RESTRICTED material within the Department. If it is necessary for the Division of Coordination and Review (CR) to review the material, it will be sent through CR.

c Outside the Department (Not to a Foreign Service Post). RESTRICTED material may be transmitted outside of the Department by the regular mail and messenger service of the Department, by the messenger service of other Departments or Agencies, or by ordinary mail, provided it does not pass through the mail service of any foreign government.

IX CUSTODY AND STORAGE OF CLASSIFIED MATERIAL.

A Custody.

1 Each custodian of classified material will exercise vigilance and initiative in applying the basic rules governing the use, handling and storage of classified material.

2 When an officer delegates authority to personnel under him to handle and have custody of TOP SECRET, SECRET, CONFIDENTIAL or RESTRICTED material, he will not consider himself relieved of the responsibility of insuring that the material so entrusted is properly safeguarded.

B Storage. The term *storage* as here used, refers to the physical or mechanical means or other security measures taken to protect classified material outside of working hours, or to the manner in which it is protected during working hours when not under the personal supervision of the individual to whom it was issued.

1 Within the Department, TOP SECRET material will be stored in vaults, safes, or steel safe-file cabinets equipped with three-combination lock or will be under protection of a means specifically approved by the Security Officer of the Department.

2 Within the Department, SECRET material will be stored in a manner authorized for TOP SECRET material or in steel file cabinets equipped with a steel bar and lock set, or in steel file cabinets equipped with plunger-type

201.1

IX B 2 (Continued)

lock and supplemented with *wonder* locks, provided the keys to locks of such files are stored behind a three-combination lock and carefully accounted for to insure against unauthorized duplication. Other means for storing SECRET material must be authorized specifically by the Departmental Security Officer.

3 Within the Department, CONFIDENTIAL material will be stored in a manner authorized for the storage of TOP SECRET or SECRET material, in metal file cabinets equipped with *either* plunger type or *wonder* locks, or in a manner specifically authorized by the Departmental Security Officer.

4 Both within the Department and the Foreign Service RESTRICTED material will be stored in the best practicable manner insuring a reasonable degree of security. A reasonable degree of security is defined to mean protection from easy access or view by persons outside of the government. Authorized containers for RESTRICTED material include file cabinets, desks, bookcases, supply cabinets, or other containers located in a building, protected by building guards. In buildings not protected by building guards, RESTRICTED material will be stored out of sight in a locked room or in a locked container.

5 At Foreign Service Posts TOP SECRET material will be stored in vaults, safes, or steel file cabinets equipped with three-combination lock. SECRET, and CONFIDENTIAL material will be stored in vaults, safes, or steel file cabinets equipped with three-combination lock or in steel file cabinets equipped with *bar and lock set* with American made locks or by other means, approved by the Security Officer of the Post concerned, which affords equivalent security.

6 Where steel file cabinets equipped with plunger type locks are used, care will be exercised to insure that all drawers are properly caught when closed and that drawers cannot be opened by applying pressure upon them in any direction when the cabinets are locked. Where *wonder* locks are used, care will be exercised to insure that drawers are closed in such a manner as to be level with the front of the file cabinets and that *wonder* locks are pushed forward on their supporting bars as far as possible.

7 Keys to plunger type, *wonder*, and other types of key locks (except door locks) will be stored behind a three-combination lock. They *will not* be carried on the persons of individuals. Any duplication of keys required will be made *only* by the Security Officer at Division, Office, FS Post, or higher levels. A report will be made to the Department Security Officer of all such keys duplicated. Keys to doors will be left in custody of building guards after working hours.

8 The name, address, and telephone number of each person knowing the combination of a safe or safe file will be entered on a list pasted on the outside front of the safe or safe file cabinet. A similar list of personnel responsible for locking file cabinets equipped with plunger-type or *wonder* locks or padlocks will be posted on the outside front of the file cabinets.

9 The combination of each safe will be changed at least once a year, and at such other times as necessary (as when any person knowing the combination severs his connection with the office in which the safe is located).

201.1

IX B 9 (Continued)

Combinations of all safes and safe-files in their respective areas will be handled as SECRET information and will be kept on file by the Security Officers of Divisions, Offices, Foreign Service establishments, and higher authorities. A duplicate copy of the combinations of all Departmental safes will also be filed in the office of the Security Officer of the Department.

10 If a safe or file cabinet is found unlocked by a building guard during his evening inspections, he will immediately telephone the first person whose name is posted on the safe or file cabinet, or other persons listed, and guard the safe or cabinet until the individual concerned reports to the office and inspects the unlocked safe or file cabinet to determine if any material is missing. Classified material found outside a storage place by the guards or other inspectors will be locked in the most conveniently located place possessing adequate security or placed under guard until delivered to the Departmental Security Officer. A report of unlocked safes or file cabinets or classified material not properly stored and of the action taken by the building guards will be made to the Security Officer of the Department on the morning following the occurrence.

C Removal of Official Material from the Department.

1 TOP SECRET. No officer or employee of the Department of State will take TOP SECRET material from the Department except for the conduct of official business. Under no circumstances will TOP SECRET material be removed from the Department outside of working hours except where official conferences or consultations are involved. Specific approval *in writing* by Directors of Offices or higher authorities will be given for such use of TOP SECRET material and copy of the authorization for removal will be filed by the TOP SECRET Control Officer of the office concerned. The date of return of the material to the office concerned will be entered upon the written authorization for removal which is held by the TOP SECRET Control Officer.

2 SECRET AND CONFIDENTIAL.

a Normally SECRET and CONFIDENTIAL material will not be removed from the Department for purposes of working with it outside of office hours. However, in case of necessity an officer may remove SECRET or CONFIDENTIAL material from his office for such purpose if permission has been granted by the Chiefs, or their deputies, of Divisions or higher levels. For such cases, there will be maintained in the office of the approving authority, a permanent registry record of the material removed, describing the material, and giving the date of removal, the name of the officer removing the material, the name of the officer authorizing removal and the date of return. The officer removing material will certify that he will assume responsibility for protecting the material in a manner commensurate with its classification.

b An inspection of such registers will be made regularly by the Security Officer of the Department.

3 RESTRICTED. Material classified RESTRICTED (except copies of classified telegrams bearing the notation "paraphrase before communicating*****", which will be handled as prescribed for SECRET) may be removed from the Department outside of regular office hours provided means are available to insure a reasonable degree of security for the material.

201.1

IX C (Continued)

4 Classified material removed from the Department will not be read or revealed in a public place.

5 Any material removed from the Department will be returned as soon as practicable to its proper place within the Department.

D Action on Resignations.

1 When an employee resigns, or otherwise severs his connection with the Department of State or Foreign Service, all classified material in his custody, his identification pass, and all Departmental keys in his custody will be turned in to the Department. Classified material which must be turned in includes personal files and any other types of material which contain classified information. Prior to giving final clearance for an employee to receive his termination pay, his immediate supervisor will be responsible for insuring that all classified material, identification passes and keys, in custody of the employee concerned have been turned in.

X OFFICE SECURITY.

A Designation of Officers to Enforce Security Measures. The Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities will designate a person in their respective organizational units (normally the Executive or Administrative Officer) to be responsible for enforcing security measures within their respective offices. In large offices, where it is not possible for one person to maintain effective supervision over all classified material, an additional employee or employees will be designated (to be known as Assistant Division, Office, or Mission Security Officers) in each room or group of rooms to assist in seeing that all classified material is properly handled during the day and properly stored when the office is closed. Designating additional employees as Security Officers and Assistant Security Officers will not relieve the Division Chief, Office Director, Officers in Charge of Foreign Service establishments, or higher authority of the responsibility of insuring that all material entrusted to the organizational unit under his jurisdiction is properly safeguarded.

B Handling Classified Material During Working Hours.

1 TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED material will not be left on desks or otherwise exposed in an unoccupied office. When it is necessary to leave an unoccupied office, classified material will be stored as indicated in paragraph IX B.

2 INSPECTION BY UNAUTHORIZED PERSONS. Employees using classified material will take every precaution to prevent deliberate or casual inspection of it by unauthorized persons. One effective precautionary measure is to keep the papers face down or covered when not in use directly; another is to have a conference table located near the entrance to the office where the officer can interview visitors. These and other such practices will provide safeguards against the possibility of unauthorized persons seeing classified material. Only those persons who must handle the material for processing or appropriate action will be permitted to see it.

201.1

X B (Continued)

3 CARBON COPIES, STENOGRAPHIC NOTES, ETC. All the rules prescribed herein for safeguarding other classified material will apply also to such items as copies of classified official documents and any informal materials, such as memoranda, rough drafts and shorthand notes, carbons and carbon copies, which contain classified information.

4 Within the Department, a report will be made to the Departmental Security Officer, through the appropriate Division, Office, or higher level Security Officers, of improper security preparation, safeguarding or transmission of classified documents. A similar report will be made to Foreign Service establishment Security Officers by employees of Foreign Service establishments.

5 A registry system will be established in organization units of Divisions, Offices, Foreign Service establishments, and higher level offices, to control effectively TOP SECRET, SECRET, and CONFIDENTIAL material processed by those organizational units.

6 Classified material will not be delivered to desks in unoccupied rooms. At the close of working hours, all document baskets will be carefully checked to insure that deliveries of classified material have not been made to desks of absent personnel.

7 A security plan will be devised by the Security Officers of organizational units to insure that proper security measures are observed during office moves. Such security plan will include provisions for assuring that containers of classified material are securely locked, clearly and distinctly addressed, and a means provided for accounting for their dispatch and receipt by responsible persons. While in transit, they will be accompanied by responsible persons.

8 Carbon paper, which has been used in typing hectograph sheets, mimeograph stencils, and tissue sheet copies of classified material, will be handled and stored in a manner commensurate with the security classification of the original of the material involved.

C Safeguarding Classified Material After Working Hours. All classified material will be removed from desks and trays and placed in storage for the night in accordance with the storage rules prescribed in Paragraph IX B. The Security Officers of Divisions, Offices, Foreign Service establishments, or higher levels will cause to be instituted a system of security checks at the close of each working day to insure that the persons responsible for classified material are properly carrying out their duties and to check on the locking of safes and file cabinets.

XI DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL.

A Destruction of Classified Material. The general rule for the destruction of all classified material is that it will be carefully and completely burned in the presence of responsible persons. Disposable classified material comprises information copies of telegrams and airgrams, memoranda, extra copies, rough drafts, shorthand notes, carbon papers, and any other non-record material which contains classified information.

201.1

XI A (Continued)

CAUTION: Classified *record* copies of official material will *not* be burned or otherwise destroyed. Classified material will *not* be deposited in ordinary wastebaskets.

B Destruction Procedure in the Department.

1 All classified waste material to be disposed of will be torn into small pieces and placed in paper containers designated as *burn-bags*. Outside of regular working hours partially filled burn-bags will be stored in a manner affording protection commensurate with the classification of material to be burned (see paragraph IX B). Burn-bags will be sealed by stapling when filled and clearly and distinctly marked *Burn*.

2 Responsible persons within each Division, Office or higher level office will be designated to deliver filled burn-bags to designated custodians at one of the collection points listed in Departmental Regulation 201.2 in accordance with the collection schedule indicated therein.

3 a Responsible employees of the Division of Central Services (CS) have been designated to collect the filled burn-bags at the locations designated. Until completely burned in the presence of a responsible person all such material will be protected by security safeguards commensurate with the classification of material involved.

b Except for classified material originated by the destroying officer, a record of material destroyed will be maintained in the office in which TOP SECRET, SECRET, and CONFIDENTIAL material is torn up and placed in *burn-bags*. The Chief of each Division, Office, and higher level office will be responsible for establishing such a record of destruction suitable to his operation and one which will enable responsibility to be fixed in cases of wrongful destruction. The Security Officer of the Department will, upon request, assist in devising a procedure for recording destruction of TOP SECRET, SECRET, and CONFIDENTIAL material in organizational units of the Department. From time to time the Security Officer will inspect records of classified material destroyed in organizational units.

C Destruction Procedure at Foreign Service Posts. The procedure to be followed at Foreign Service Posts for destroying classified material will be prescribed by the Security Officer of the Post concerned and will be in accordance with the principles outlined in paragraphs XI A and B above. Persons witnessing the destruction of classified material must be United States citizen employees. A record of TOP SECRET, SECRET, and CONFIDENTIAL material destroyed will be maintained at each Foreign Service Post. Such records will be inspected periodically by the Security Officer at each Post.

XII DEPARTMENTAL BUILDING SECURITY.

A Since pass control systems are not in general operation to restrict entrance into State Department Buildings during working hours, extreme care must be exercised by all officers and employees handling classified material during the day. Such material will be safeguarded at all times as prescribed in paragraph X B above, which prescribes regulations for handling classified material during working hours.

XII (Continued)

B Pass controls are in operation after working hours and employees are required to present identification passes to the guards and to sign a register when entering or leaving any Department of State building outside of regular working hours. Employees who do not voluntarily present identification passes to guards after working hours will be specifically requested by the guards to show their passes.

C Visitors will not be permitted in any Department of State building after working hours, unless they are escorted in and out of the building by an employee from the office of the person on whom they are calling or unless the building guard is authorized to admit the visitor by the person on whom the visitor is calling.

D All keys of office doors kept locked after working hours will be turned in to the building guards to be held in their custody after working hours.

XIII CRYPTOGRAPHIC SECURITY. The following regulations, in addition to those prescribed in Sections I through XII above, are concerned with the safeguarding of cryptographic material and are designed to assure a high degree of cryptographic security in the Department and the Foreign Service.

A Drafting Classified Telegrams.

1 Each telegram will be drafted to be as brief as is consistent with clarity and completeness.

2 Punctuation will be held to a minimum. Prepositions, pronouns, parts of the verb *to be*, and articles (particularly *the*) will be omitted where possible. Recognized or authorized abbreviations may be substituted for the complete words where they would be readily understood by officers of the Department and the Foreign Service. In referring to previous telegrams, the hour designation is necessary only to identify circular telegrams.

3 Set forms of expression and repetitious phraseology will be avoided in drafting telegrams with similar texts to prevent the compromise of a cryptographic system through similarities in the resulting encrypted texts. The necessity for repeating the same basic text with only minor changes in each telegram can often be avoided by including the information for all addressees in one multiple-address telegram, or by substituting words such as *the country to which you are accredited* for individual names. In other cases one telegram may be repeated to all addressees containing the identical information and a separate telegram may be sent to each addressee with the different information. If other methods are not applicable, paraphrasing will be employed to vary the phraseology of telegrams which would otherwise be drafted with long identically worded passages.

4 Words and expressions commonly used will be avoided at the beginnings and endings of telegrams. A deliberate attempt should be made to conceal in the text a direct reference to a previous communication, an internal address or signature, and routing or delivery instructions. Commonly used words which should not appear as the first word of a telegram are: Dept., Embassy, Legation, Please, and Following. Commonly used last words to be avoided are: advise(d), follow(s), informed, urgently, and (un)quote. The first or last word of a telegram should not be the name or nationality of the country or place to which the telegram is addressed or from which it is sent.

201.1

XIII A (Continued)

5 Two separately numbered telegrams will be sent in preference to one long telegram involving only a small amount of classified information. The classified telegram may refer to the plain language telegram, but the reverse is never permissible.

6 Whenever the drafting officer knows that the information in a classified telegram has been or may be communicated to persons other than American employees of the U. S. Government he will indicate this fact or possibility by the marking VERBATIM TEXT at the top of the telegram as explained in paragraph V C 5 a.

7 Originators of classified telegrams in the Department will prepare only the number of copies desired by the Division of Communications and Records (DC), plus one copy for retention until a confirmation copy is received from the Division of Communications and Records (DC).

B Classification of Telegrams.

1 The Officer drafting a telegram is responsible for indicating its correct security classification.

2 The classification of each telegram must be given careful consideration since over-classification and under-classification are equally to be avoided.

3 Each telegram making a direct reference by subject matter or other identifying information to a telegram classified CONFIDENTIAL or higher will be classified at least CONFIDENTIAL. Each telegram making a direct reference to a telegram classified RESTRICTED will be classified at least RESTRICTED. An UNCLASSIFIED telegram will not contain a direct reference to a classified telegram.

4 The security classification will be clearly indicated on the top and bottom of the hectograph copy prepared and on each sheet or copies thereof. If classified TOP SECRET, the abbreviation TOPSEC will also be placed in the text near the beginning.

C Transmission of Classified Telegrams.

1 True readings of classified telegrams will be distributed within an establishment only by the Message Center. When it is desired that other offices receive information copies of such telegrams the Message Center (Code Room) will be notified and copies forwarded through normal channels.

2 The serial identification number, as well as any serial numbers used within the text as references to other classified telegrams, will be deleted before a classified telegram is communicated to any one outside the United States Government service. Every possible effort will be made to disguise the fact that the text communicated was taken from a telegram.

3 If it is essential that the contents of a classified telegram be transmitted by mail or messenger to another establishment in true reading form, it will be transmitted with the safeguards applying to SECRET material, unless

XIII C 3 (Continued)

it is TOP SECRET, in which case it will be transmitted with the safeguards applying to TOP SECRET material. (see also paragraphs V C.5 b and c).

4 The transmission to another establishment by mail or messenger of copies of the plain text of encrypted telegrams for confirmation purposes is strictly prohibited.

D Paraphrasing.

1 Paraphrasing is employed as a protective measure for certain cryptographic systems.

2 The text of a telegram will be carefully paraphrased when the copy distributed is marked "Paraphrase Before Communicating*****" and the information therein is to be communicated to persons other than American employees of the U. S. Government. The paraphrased version transmitted will not show the serial number of the original telegram or the serial numbers of any classified telegrams used as references within the text.

3 When paraphrasing is employed all of the following processes will be applied to the text of the message:

- a Change the order of the paragraphs.
- b Alter the position of the sentences in each paragraph.
- c Shift the positions of the subject, predicate and modifiers in each sentence.
- d Substitute synonyms or equivalent expressions, but exercise care to assure that confusion of meaning does not result.
- e If the above-mentioned steps have not changed the length of the paraphrased version try to use other phrases, clauses, and synonyms in order that the paraphrased text will vary at least 15 per cent from the original text.

E Use of Cryptographic Systems.

1 No cryptographic system will be used unless it has been issued or approved by the Chief of the Division of Cryptography (CY) of the Department.

2 The number of persons allowed to have knowledge of the Department's cryptographic systems will be limited to those requiring such information for the performance of their duties.

3 The following persons are authorized to see and make use of cryptographic material when their duties require a knowledge of cryptographic operations; commissioned officers of the Foreign Service and specifically designated employees of Missions approved by the Chief of the Division of Cryptography (CY) and the Security Officer of the Department; specifically designated employees of the Division of Communications and Records (DC); employees of the Division of Cryptography (CY); and the Security officer of the Department and of each Foreign Service Post.

201.1

XIII E (Continued)

4 Only United States citizens will be authorized by the Security Officer of the Department to perform cryptographic work and have access to the Department's cryptographic systems.

5 No one will be permitted to encrypt messages for transmission until he is thoroughly familiar with security regulations in general, the Cryptographer's Manual, and the detailed instructions provided for the operation of the cryptographic systems concerned.

6 A clerk recruited locally at a Foreign Service Post will not be assigned to cryptographic duties until he has served at that post for at least six months, and approval of the Department obtained or indicated in paragraph 3 above.

F Special Rules for Safeguarding Cryptographic Material.

1 Careful consideration will be given to the location and arrangement of code rooms and openings thereto in order to prevent the viewing of exposed cryptographic material by unauthorized persons. Only those persons whose duties require access to the Code Room will be allowed to enter it. A notice will be prominently displayed on the outside of the door to the Code Room with the following words on it, *RESTRICTED AREA - NO ADMITTANCE*.

2 When it is necessary for unauthorized persons to enter the Code Room, such as for cleaning or building maintenance, all cryptographic operations will be stopped and the cryptographic material will be stored as required for unattended material or it will be covered and guarded.

3 Cryptographic material to be transmitted to or from the field will be securely wrapped in heavy paper, will be sealed or tied, and marked *SECRET*, and the package will then be transmitted via Diplomatic Fouch facilities.

4 Cryptographic material will be stored in a three-combination safe or safe file or in a manner which provides equivalent security and which has been approved by the Departmental Security Officer, or the Security Officer at the Foreign Service establishment concerned.

5 All vaults and safes containing cryptographic material will be locked when the room in which they are located is left unguarded.

6 A destruction plan will be formulated by all custodians of cryptographic material and necessary material will be readily available to effect the complete and total destruction of cryptographic material in the event of an emergency. Destruction plans will include burning, smashing equipment with heavy instruments, and any other action designed to render cryptographic material unrecognizable and insure its complete destruction.

7 On suspicion or evidence that unauthorized persons have obtained possession of or copied elements of a cryptographic system, its use will be discontinued at once and the Department will be notified as to the elements concerned and advised whether the compromise is certain, probable, possible or improbable.

XIII (Continued)

G Responsibility for Cryptographic Security.

1 The Chief of the Division of Cryptography (CY) is the Cryptographic Security Officer for the Department and, in collaboration with the Security Officer of the Department is responsible for the formulation of all cryptographic security rules to be observed in the Department and in the field.

2 The officer personally responsible for the issuance and enforcement of cryptographic security rules at each Foreign Service Post will be known as the Cryptographic Security Officer. Although the Officer in Charge is responsible for cryptographic security, he may designate another officer assigned to the post to act as Cryptographic Security Officer.

3 The Cryptographic Security Officer will be the Custodian of cryptographic material issued to his post. In the Department the Officer in Charge of the Telegraph Branch will be the Custodian of cryptographic material issued for current use by the Telegraph Branch and the Chief of the Division of Cryptography will be the Custodian of all other cryptographic material.

4 A daily check on the status of cryptographic material will be made at each office. Each person in a responsible position where cryptographic material is used under his supervision will maintain a daily record or keep a running inventory of all such material as it is removed from its storage place during each work day or shift. If this record or inventory discloses the loss of any material, a careful search will be started at once and a report of the circumstances will be made forthwith to the Cryptographic Security Officer directly concerned. After investigating and evaluating a loss, the Cryptographic Security Officer will make a report to the Department (Division of Cryptography (CY)).

5 On January 1 and July 1 of each year the Cryptographic Security Officer will cause an inventory of all cryptographic material in his custody to be made by two officers (one officer at posts having only one assigned) and a list of this material by Short Titles and register numbers will be forwarded to the Department, Division of Cryptography (CY). (Foreign Service Form 345).

6 When cryptographic material is destroyed the destruction will be witnessed by two officers (one officer under unusual conditions of necessity - explanation of such conditions will be submitted with the report of destruction) and a report signed by these officers listing the Short Titles and register numbers of this material will be submitted to the Department, Division of Cryptography.

7 When a permanent transfer of officers takes place, the officer assuming charge will submit to the Department, Division of Cryptography, an inventory report listing the Short Titles and register numbers of the cryptographic material on hand. (Foreign Service Form 345).

INDEX TO SECURITY REGULATIONS OF THE DEPARTMENT OF STATE

- A -

Access	
to classified material	VIIA, B, C2, 3; XB2
to Code Room	XIIIF1,2
Accumulated Files	IVB2
Additional safeguards, for transmitting	
Top Secret Material.	VIIIB
Address, in classified telegrams.	XIIIA4
Addressing, classified material	VIIIB1b (3), c (1), (3), d (2), (3), 2a (8), b (1), (3), c (2), 3a (4), b (4), 3c (2)
Administrative Officers	
as security enforcement officers	XA
keep safe combinations on file	IXB
responsible for controlling distribution	VIIIB2
Airgram	
containing quotations from telegrams	XIIIC3
true reading of.	IC12
Airgram Service, unclassified material in	IIA
Approving Officer	IVA
Attaching receipts.	VIIIB1b (4), c (3), d (2), e (3), (9), 2c (3)
Authority	
for custody of classified material	IXA
for publication abroad	VIE
to approve security classifications.	IVA
to classify.	IVA
to declassify or downgrade	IVB2,3,4,5
to downgrade or declassify classified material of foreign nations.	IVB3
to give testimony.	VIF
to make public classified information.	VIC, D, E
Authorization	
for removal of classified material	
from Department.	IX C
to see classified material	VIIA, B, D2
to see Top Secret material	VIIC
to use cryptographic system.	XIIIE

- B -

Baskets, document check of.	XB6, C
Books, classification of.	VB3
Burn Bags, procedures in use for.	XIB
classified waste	XIB
Cabinets, for storage of classified material (see also containers, safes).	IXB
Cancelling or changing, classifications	IVB

Carbons, as classified material. IC1, XB3,8, XIA

Careless talk. VIB

Certification for access to
Top Secret. VIIIB1e(2)

Classified Material

 changing classification of. IVB

 custody IXA

 definition. IC1

 Destruction, disposal XIB

 dissemination and distribution. VA3, VID, VII

 downgrading and declassifying IIF, IVB

 extracts from IIB

 knowledge of. VIIA

 marking of. VB,C

 of defunct Agencies IVB4

 of foreign Agencies IIG, IVB3

 of other Agencies IIG, IVB4, VA4, VIID2

 outside of storage place. IXB

 possession of VIIA

 preparation of. VA, XB4

 protection of IC14, VI

 publication of. VIC

 removal from Dept. IXC

 reproduction of VA

 requests for. VIIB2, VIID1,3

 responsibility for. VIA, XA, B, C,

 return of to Dept. IXC5

 review of assigned classifications. IVA4

 right to receive. VIIB

 safeguards. XB, C

 stencils. XB8

 storage IC14, IXB, XC

 telegrams XIII A

 tissue sheet copies XB8

 transmission of VIIIB

Collection Points, for classified waste. XIB2

Confidential information, material

 definition of and examples. IIIC

 dissemination, distribution VIIA, B, D, VIIIB3

 storage IXB3

 transmission of within Dept. VIIIB3a

 transmission of, within
Foreign Service Post. VIIIB3a

 transmission of, outside Dept. VIIIB3c

 transmission to Foreign Service Post VIIIB3b

Containers, for storage of classified material IXB, XC, XIB

Control Officer for Top Secret material. VIIIB1e

Copies of classified material. VA, B, VIID1, XB3,8,
XIA, XIII A7, XIIIB4

Copies, confirmation; of telegrams XIIIIC3

Courier System for transmission of Top Secret. VIIIB1c(4), d(1)

Cryptographic Materials

 classification of IIIB1f, C2f

 definition. IC3

 destruction XIIIIF6

 rules for safeguarding. XIIIIF

Cryptographic Security	
definition	IC4
responsibility for	XIIIIG
Cryptographic System	
compromise of	XIIIIF7
definition	IC5
protection of	XIIID, F
Custodian	
of classified materials	IXA
of cryptographic materials	XIIIG3
Custody	
of Secret, Confidential, Restricted material	IXA
of keys	IXB7, D
of Top Secret material	VIIIB1a(2)

- D -

Declassifying and Downgrading	IC6,8, IIF, IVB
automatic	IIF
authority to	IVB
foreign material	IVB3
material of Other Agencies	IWA4
procedure	IVB7
Declassification Committee	IVB8
Departmental Security Officer, authority and responsibilities	VIIIB2c(1), 3a(1), IXB2,3,7 XB4, XIB3b, XIIIG1
Destruction, destroying	
of classified material	IA, XI
of cryptographic material	XIIIF6
record of	XIB3b
Disposal	
of classified material	XI
of classified telegrams	XI
of classified waste material	XI
of wastage from reproduction	XI
Dissemination and distribution, of	
classified material	VA3, VIIB,C
outside the Department	VIID
Top Secret	VIIC
of classified telegrams	XIIIC1

- E -

Executive Officers, security responsibilities of	VIIB2, IXB7,9, D,X
Extracts, from classified documents	IIB2

- F -

File of documents	
classification of	IIId
marking of	VC4
Functions of Security Officers of organizational units	XA

- 0 -

Grading of official material (see classified material)

- H -

Handling, classified material. VIIC2, IA, VIID4, VIII, XB

- I -

Identification Pass, presentation of XIIB
Initials, on record copy IVAL, 2, VIID1, VC3

- K -

Keys

duplication of. IXB7
protection of IXB2
storage outside of working hours. IXB7

- L -

Locking doors outside of working hours XIID
Loose File, marking of VC4

- M -

Marking

burn-bags XIB1
classified material VB, C,
cryptographic materials XIIIF3
envelops. VIIIIB
loose files VC4
material disseminated to
private entities. VC1
security classification on
cover envelops. VIIIIB
"Verbatim Text" on telegrams. VC5
Messages, changing classification of IVB6 (b), (c)
Moves, office; security during XB7

- N -

Notations, on classified material. VB, C, VIID4

- 0 -

Office Security. X
Other Government Agencies
classified material from. IIG, VIID2, VIIIIB2a (6)
declassification, downgrading of
material from IVB4
distribution to VIID1
transmission of classified material to VIIIIB1d, VIIIIB2c,
VIIIIB3c, VIIIIB4c
use of courier (messenger) service of VIIIIB1d, VIIIIB2c,
VIIIIB3c, VIIIIB4c
Overclassification IIE

- P -

Pages, marking of. VB
 Pamphlets, marking of. VB3
 Paraphrased Telegrams.
 marking of. VB2, VC5c
 transmission of VD, VIIIA1
 Paraphrasing IC10, XIIIID
 of extracts from telegrams. IIB2, XIIIID
 of telegrams. IVB6 (b), (c), VB2, XIIIID
 rules for XIIIID
 Pass Control System. XII
 Personnel
 leaving employment of Department. VIH, IXD
 Security instruction of VIG
 Physical Security, responsibility for. VIA
 Preparation of classified material V
 Publication, security rules for. VIC, D

- R -

Receipt System
 for Confidential material VIIIIB3
 for Secret material VIIIIB2
 for Top Secret material VIIIIB1
 Record of destruction XIB3b, c
 Record Copies. IVA1b, 2b, IVB6a, VC3,
 XIA
 Records, of material distributed VIID, VIIC3, VIIB2,
 XB5
 References
 to classified material, (including
 via telephone). VIIIA2, IIB2
 in telegrams. XIIIIA2, 4, 5, XIIIIB3
 Registered Mail, used for transmitting
 classified material VIIIB1a (3), VIIIB2c (1),
 VIIIB3c (1)
 Registry System, for classified material XB5
 Release, of classified material. VIC, VIID3
 Reproduction, security rules for VA, VB
 Responsibility
 for enforcement of security VIA, X, XA, XIIIG
 for material in custody of persons
 leaving employ of Department. VIH, IXD
 for safeguarding. VIA, IXA, XC, XIB, XIIIG,
 XIIA
 for security of information VIA
 Restricted material, information
 communicated via telephone. VIIIA
 definition and examples IIID
 dissemination, distribution of. VIIB
 in testimony. VIF1
 procedure of classification IVA3
 storage of. IXB4

telegrams.	XIIIB3
transmission of.	VIIIB4
true reading.	IVB6(c)
Reviewing of classified material.	IIIE1, IVA

- 8 -

Safeguarding	
classified material outside of working working hours.	XC
cryptographic materials.	XIII
transmission of classified material.	VIIIB
Safes, storage of classified material in.	XB, XIB1
Secret material	
classification procedure.	IVA2,3
control by registry system.	IXC2, XB5
definition and examples.	IIIB
destruction of.	XIB
dissemination, distribution.	VIIIB2
receipting for.	VIIIB2
registering of.	VIIIB2a (2), IXC2, XB5
removal of from Dept.	IXC2
storage of.	IXB2, 5, XB, C
telegram.	VIIIB2a (3), XIIIC2
transmission of.	VIIIB2
Security	
daily inspections.	XC
plan for moves.	XB7
Security Classification (see classified material)	
Security Messenger Service.	VIIIB1b (1), (3), (4), d (1), (2)
Security Officers, functions	
Department Security Officer.	IVA4, B2, 4, 8, VIIC2, D3b, c, VIIIB1b (5), d (1), IXB, XIIIG
Organizational Unit Security Officer.	XA
Security procedures, instruction in.	VIG
Special marking.	VB, C
Storage, of classified material.	IC14, VIID4, IXB, XB, C, XIB1, XIIIF4,5
System of Security Checks.	XC

- 9 -

Telegrams	
as classified material.	IC11, XIA, XIIIA, B
classification of.	XIIIB
definition.	IC11
disposal of copies.	XI
distribution.	VIIIB1, XIIIC
downgrading.	IVB6
drafting.	XIIIA
indicating classification of.	VB
paraphrased versions.	IIB2, IVB6
paraphrasing.	XIIID
transmission of true reading.	XIIIC3

Telephone, use of for classified information. VIIIA

Tissue Sheet Copies, handling and storage of. XB8

Top Secret material, information as a classification IIIA

certification for access to VIIIB1e

Classification procedure. IVA1

Control Officer VIIIB1e, IXC

definition and examples IIIA

destruction, disposal of. XIB

distribution outside Department handling. VIIC, D, VIIIB1d

marking VIIC, VIIIB1, XB, C

protection of VC3, VIIIB1

storage IXA, XB

testimony IXB1, 5

VIF2

Transmitting, transmission, of classified material VIII, XIIIC, F3

between organizational units. VIIIB1b, 2a, 3a, 4a

Security Messenger Service (see Security Messenger Service)

confidential material VIIIB3

outside Department. VIIIB1d, 2c, 3c, 4c

restricted material VIIIB4

secret material VIIIB2

to Foreign Service Post VIIIB1c, 2b, 3b, 4b

to other Government Agencies. VIID, VIIIB1d, 2c, 3c, 4c,

VIIIB1

Top Secret material VIIIB1c (4), 2a (4), b (4)

via Diplomatic Courier. VIIIB2, 3a, 4a, c

via regular Messenger Service VIIIB1a (1), b (1), (2), (4), 2a (1), (2), (4), 3a (1), 4a

via responsible personnel VIIIB1b, 2a, 3a, 4a

within Foreign Service.

- U -

Unclassified material, information marking IIA

telegrams IIIIE, XIIIA5

Upgrading, definition of IC13

- V -

"Verbatim Text", marking on telegram VC5

Visitors, outside of working hours XIIC

- W -

Waste baskets, prohibited for disposal of classified material. XIA

Waste material, classified disposal of XIB



DEPARTMENT OF STATE

REFERENCE MANUAL
SECURITY REGULATIONS

FOR OFFICIAL USE ONLY

REFERENCE MANUAL
ON
SECURITY REGULATIONS

Prepared by Direction
of

Donald Russell

Assistant Secretary for Administration

REFERENCE MANUAL
ON
SECURITY REGULATIONS

This Reference Manual on Security Regulations has been provided as a handy reference copy of security regulations applicable to the Department and the Foreign Service. Keep this manual in your desk and refer to it frequently for guidance in respect to security practices and procedures to be employed. The contents of this reference manual are included also in the Administrative Manual as part of the Departmental Regulations.

All Departmental and Foreign Service personnel are required to read and understand the security regulations contained herein. A statement to this effect will be submitted to the Security Officer of the Department through the Security Officers of the various organizational units.

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

- I. GENERAL
- II. EXAMINATION AND CLASSIFICATION OF MATERIAL
- III. CATEGORIES OF CLASSIFIED MATERIAL
- IV. AUTHORITY TO CLASSIFY, APPROVE CLASSIFICATIONS AND DECLASSIFY OFFICIAL MATERIAL
- V. PREPARATION, REPRODUCTION AND MARKING CLASSIFIED MATERIAL
- VI. RESPONSIBILITY FOR SAFEGUARDING CLASSIFIED MATERIAL
- VII. DISSEMINATION AND DISTRIBUTION OF CLASSIFIED MATERIAL
- VIII. HANDLING AND TRANSMISSION OF CLASSIFIED MATERIAL
- IX. CUSTODY AND STORAGE OF CLASSIFIED MATERIAL
- X. OFFICE SECURITY
- XI. DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL
- XII. DEPARTMENTAL BUILDING SECURITY
- XIII. CRYPTOGRAPHIC SECURITY

201.1

201.1 SECURITY REGULATIONS OF THE DEPARTMENT OF STATE. (Effective 1-1-47)

I GENERAL.

A The purpose of this regulation is to prescribe the security rules for classifying or grading, marking, reproducing, handling, transmitting, disseminating, storing, and destroying official material originating in or coming under control or jurisdiction of the Department of State and the Foreign Service.

B Official ~~material~~ ^{info} (originating in or coming under jurisdiction of the Department of State and the Foreign Service) is of varying degrees of value to all nations, including any potential enemies of the United States, both internal and external, and, therefore, requires corresponding degrees of protection to prevent disclosure to unauthorized persons. Official material must be examined and, if protection is required, classified (or graded) in accordance with the degree of protection deemed necessary. The definitions and policies stated in this regulation are to insure the accurate and uniform classifying or grading and appropriate protection of official material.

C Definitions.

1 CLASSIFIED MATERIAL. Classified material refers to official material containing information to which a security classification has been assigned. As used herein, it also includes copies of official documents and any other official materials such as letters, instructions, memoranda, telegrams, airgrams, despatches, reports, notes, rough drafts, shorthand notes, carbons, and carbon copies which contain classified information.

2 CLASSIFYING OR GRADING. Classifying or grading includes rendering a decision relative to the degree of safeguarding required for a particular item of information and the act of stamping or otherwise marking, with an indication of one of the prescribed security classifications, the physical form in which the information appears.

3 CRYPTOGRAPHIC MATERIAL. Cryptographic material includes all documents and devices employed in changing plain-language messages into unintelligible form by means of codes and ciphers.

4 CRYPTOGRAPHIC SECURITY. A general term denoting the provision of technically sound cryptographic systems, their proper use, and their careful safeguarding.

5 CRYPTOGRAPHIC SYSTEM. Code and/or cipher ^{device} and instructions therefor.

6 DECLASSIFYING. The act of removing entirely a previously imposed security classification, thus making the information involved *unclassified*.

7 DOCUMENTS. Any form of recorded information. The term *document* includes printed, mimeographed, typed, photostated, and written matter of all kinds; despatches, instructions, telegrams, memoranda, reports, minutes, airgrams, charts, maps, drawings, notes, or photostatic copies; photographs and photographic negatives; and all other similar matter.

201.1

I C (Continued)

8 DOWNGRADING. The act of lowering the assigned security classification of classified documents and material.

9 OFFICIAL MATERIAL. Information furnished to the Department and the Foreign Service in oral or documentary form in the conduct of official government business.

10 PARAPHRASING. A restatement of text in different phraseology without alteration of its meaning.

11 TELEGRAM. Any communication sent (or intended to be sent) by electrical means.

12 TRUE READING. The unparaphrased literal text of a telegram or airgram.

13 UPGRADING. The act of changing the assigned classification of official material upward.

14 STORAGE. Storage refers to the manner in which classified material is protected by physical or mechanical means or other security measures taken to protect classified material outside of working hours, or to the manner in which it is protected during working hours when not under personal supervision.

II EXAMINATION AND CLASSIFICATION OF MATERIAL.

A Official Material Will Be Examined. All originators of official material will make a determination as to the necessity of its being placed in one of the four security classification. If a security classification is required, the material will be graded and the physical form in which it appears will be marked TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED.

Note: The term UNCLASSIFIED will be used when it is essential to convey to a recipient of the material involved the fact that it has been examined with a view to imposing upon it an appropriate security classification and that a determination has been made that the material is unclassified. It is mandatory that all unclassified material moving through the diplomatic pouch, airgram, and telegram services of the Department be marked or stamped UNCLASSIFIED.

B Classifying or Grading.

1 Persons authorized to classify official material are outlined in paragraph IV.

2 Each document will be graded or classified according to its own content and not necessarily according to its relationship to another document except telegrams referring to previously classified telegrams (see paragraph XIII B). This also applies to extracts from classified documents, except certain telegrams which bear the notation "paraphrase before communicating *****" Extracts from such telegrams will be classified the same as the telegrams from which taken unless the extracts are paraphrased. If paraphrased, such extracts may be classified according to the nature of their contents.

C Only One Security Classification. Only one security classification will be assigned to a single document or device.

(1-1-47)

(TL 39)

II (Continued)

D **File of Documents.** The classification of a file or group of physically connected documents will be that of the highest classified document contained therein. A letter of transmittal will be classified at least as high as any of its enclosures.

E **Overclassification.** Documents or material requiring classification under the provisions of these regulations will be assigned the least restrictive classification consistent with the proper safeguarding of the information or material concerned. *OVERCLASSIFICATION MUST BE AVOIDED* since it causes unnecessary delay and expense in the handling and transmission of documents, overburdens storage facilities, and depreciates the importance of classified information in the minds of handling personnel.

F **Automatic Downgrading or Declassifying.** Whenever practicable the classifying officer will place a notation on the document that upon the happening of a specified event or on a named date, the classification of the document will be reduced automatically to a stated lower classification or cancelled altogether without reference to the originating or higher authority. In the case of telegrams it will be necessary to include within the text any instructions relative to automatic downgrading or declassifying. Such instructions are in addition to the notation *Verbatim Text* required by the provision of paragraph V C 5a below. (See also paragraph IV B below).

G **Classification of Material From Other Government Agencies.** Matter obtained from the War and Navy Departments, other Government agencies, or foreign governments will be maintained by the Department and Foreign Service in the same or equivalent classification category as that in which it was placed by the originating agency.

III CATEGORIES OF CLASSIFIED MATERIAL.

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 matters in time of peace will be limited to those which in and of themselves, if disclosed without authorization, would reasonably be expected to lead directly to a definite break in diplomatic relations or to a war or have other comparatively grave consequences.

1 *Very Little Material or Information Belongs in the TOP SECRET Category.*

2 The following are some examples of material or information which normally will be graded TOP SECRET:

a Information or material regarding or details of discussions or negotiations with foreign governments on questions of great delicacy, the premature disclosure of which would reasonably be expected to lead directly to a definite break in diplomatic relations or to a war.

b Informational or intelligence material containing indications of sources of intelligence where it is of paramount importance to the United States to protect the source in order to insure a continuance of the receipt of intelligence from the sources and where the unauthorized

III A 2 b (Continued)

disclosure of the sources would cause exceptionally grave damage to the United States through the loss of intelligence from such sources or would place individuals constituting the sources in extreme jeopardy of life or limb. *Very few* intelligence sources come within this category.

c Information or material concerning the existence or details of new devices or methods of warfare of extreme importance to national security. Such information normally will be classified TOP SECRET by the military or naval forces.

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.

1 The following are some examples of official material or information which normally will be graded SECRET:

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

b Important information or material obtained from or for transmission to high levels of the Government, the premature disclosure of which might endanger the success or effectiveness of a program or policy of *great importance* to the United States Government.

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

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

e Vital information on important defenses. Such information normally will be classified SECRET by the military or naval forces.

f High-grade cryptographic devices and related material.

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

1 *The Major Portion of Information Should be Classified no Higher Than CONFIDENTIAL.*

2 The following are some examples of official material or information which normally will be classified CONFIDENTIAL:

a Important intelligence reports.

201.1

III C 2 (Continued)

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

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

d Consultative inter-Departmental communications on questions of policy where disclosure might precipitate undesirable public controversy.

e Important information or material obtained from or for transmission to high levels, the unauthorized disclosure of which would greatly embarrass the Department or the source.

f Certain cryptographic devices and related material.

D **Restricted.** Information or material which does not fall within higher categories but which should not be communicated outside the Government without adequate clearance will be classified RESTRICTED.

1 The following are some examples of official material or information which normally will be graded RESTRICTED:

a Certain economic, industrial, or political information which should not be released or communicated to the press or otherwise published and made available to the public.

b Interpretations representing official Department views and based on official or public reactions to general international or economic questions.

c Administrative or instructional communications and documents requiring the protection of a security classification, which are intended strictly for official use within the Department or the Foreign Service.

d Reports on certain internal affairs of the United States and of foreign countries which should not become public knowledge.

E **Unclassified.** Material not marked with one of the above security classifications will be understood to be UNCLASSIFIED.

1 Material not falling into one of the above classifications but which is to be forwarded by telegram, airgram, or diplomatic pouch facilities will be marked UNCLASSIFIED. This marking is not otherwise obligatory and is used only on material transmitted by one of the above mentioned facilities to assure that it has been reviewed and appropriately classified or graded.

IV AUTHORITY TO CLASSIFY, APPROVE CLASSIFICATIONS AND DECLASSIFY OFFICIAL MATERIAL.

A **Classifying or Grading.** The originator of a document will be responsible for imposing a security classification on it, as required, appropriate to its contents. The security classification imposed will be subject to the following procedures for review and approval:

201.1

IV A (Continued)

1 TOP SECRET.

a The imposition of the Classification TOP SECRET on material will require, in each instance, the personal approval of the Director of an Office, or higher authority, their respective deputies, or officers specifically designated in writing by them to act in their absence or for emergency cases. In the Foreign Service the use of the TOP SECRET classification will require, in each instance, the personal approval of the Officer in Charge, the next ranking officer or, in the case of Embassy Staffs only, the Chiefs of major subdivisions of such staffs.

b The official record file copy of TOP SECRET material, in addition to being stamped or marked TOP SECRET, will be marked with the date of classifying and the words *classification approved* adjacent to the classification mark, and will be initialed by an authorized approving officer, as indicated above, in a space provided following the words *classification approved*.

2 SECRET.

a The imposition of the SECRET classification will require, in each instance, the personal approval of the Chiefs of Divisions, or higher authority, their respective deputies, or an officer specifically designated in writing by them to act in their absence or for emergency cases. In the Foreign Service, the use of the SECRET classification will require, in each instance, the personal approval of the Officer in Charge, the next ranking officer or, in the case of Embassy Staffs only, the Chiefs of major subdivisions of such staffs.

b The official record file copy of SECRET material, in addition to being stamped or marked SECRET, will be marked with the date of classifying and the words *classification approved* adjacent to the classification mark and will be initialed by an authorized approving officer, as indicated above, in a space provided following the words *classification approved*.

3 CONFIDENTIAL AND RESTRICTED. Any originator of official material may cause such material to be classified *CONFIDENTIAL* or *RESTRICTED* as warranted by the contents.

4 The Security Officer of the Department will review, from time to time, the use of all security classifications throughout the Department and the Foreign Service in order to insure uniform and proper usage. For this purpose, he will collaborate closely with Administrative or Executive Officers of Divisions or Offices and designated Officers in the offices of Assistant Secretaries and higher levels.

B Downgrading and Cancelling Classifications.

1 It is the obligation of all officers to keep classified matter of current interest or continuing value constantly under review and to downgrade it as soon as conditions permit.

2 When it is desired to downgrade documents of the same type which accumulate in bulk, authority to downgrade or declassify in bulk will be obtained from the Security Officer.

201.1

IV B (Continued)

3 Material which has been classified solely to accord with conditions imposed by a foreign nation may be downgraded or declassified with the consent of the nation concerned or by approval of the Secretary or Under Secretary.

4 MATERIAL FROM OTHER DEPARTMENTS OR AGENCIES. Material originated in other Departments or Agencies cannot be reduced in classification except with consent of that Department or Agency. If it is desired to retain such material and to reduce it in classification, the Division should make a list of the material and send it to that Department or Agency requesting that the material be reduced in classification. Material which originated in agencies which are no longer in existence should be referred to the Security Officer, Department of State, who will take appropriate action.

5 The officer imposing the original classification, (not necessarily the approving officer), or higher authority, may cancel or change the classification of a document by writing or stamping over or adjacent to the classification mark at the top of the first page, "Classification changed to _____, by authority of (name of officer making the change, office symbol, and the date thereof)." An exception to the above is made in the case of telegrams containing the notation "paraphrase before communicating*****".

6 (a) The officer on cancelling or changing the classification of material will notify the custodian of the official Department record copy. When considered necessary and feasible, the officer effecting the cancellation or change in classification will notify all offices or personnel concerned, by memorandum, of the cancellation or change in classification of the material. Such memoranda of notification may be informal in nature, e.g. in hectographed form.

(b) In the case of telegrams marked "Paraphrase Before Communicating*****", no change in classification will be made unless the text has been carefully paraphrased and the serial number of the original telegram and any to which reference has been made have been deleted, except that messages classified TOP SECRET may be downgraded to SECRET when their content warrants.

(c) The *true reading* of a telegram marked "Paraphrase Before Communicating*****" and classified TOP SECRET or SECRET will not be reduced to a classification below CONFIDENTIAL earlier than 5 years following the date of the telegram. The *true reading* of classified telegrams may be declassified if the telegrams are over 10 years old and if the declassification action is warranted by the contents of the telegrams.

7 The *declassification and downgrading procedure* of the Department is outlined in detail in Departmental Regulation 201.3.

8 A *Declassification Committee*, consisting of the Security Officer of the Department and one representative each from the Office of the geographic area concerned with the material being considered for declassification, Office of Foreign Service (OFS), and Office of Intelligence Coordination and Liaison (OOL) will act as the final arbiter in cases where there is a lack of agreement on the downgrading or declassification of any item of information.

201.1

V PREPARATION, REPRODUCTION AND MARKING CLASSIFIED MATERIAL.

A Preparation and Reproduction of Classified Material. Classified material will be prepared with a minimum number of copies as the risk that classified material may fall into unauthorized hands increases in proportion to the number of copies in existence.

1 PRINTING OR REPRODUCTION. The Officers directing the preparation, printing, or reproduction of classified material will cause strict supervision to be exercised over the disposition of the notes, manuscripts, type, plates, stencils, negatives, and wastage incident thereto, in a manner which will properly safeguard the information being reproduced.

2 NOTATION OF REPRODUCTION. The copy of TOP SECRET, SECRET, or CONFIDENTIAL material, from which reproduction is made will contain or have attached thereto a notation relative to the authority for reproducing the material and the number of copies made.

3 DISTRIBUTION OF REPRODUCED MATERIAL. Except for Divisions of the Department authorized to make regular distribution of material, no distribution of material (classified higher than RESTRICTED) reproduced will be made outside of the reproducing Division unless specifically authorized by a responsible officer of the originating Division, or by the Chief or his Deputy of the Division having jurisdictional control over it if it originated in a Foreign Service Post.

4 MATERIAL FROM OTHER DEPARTMENTS.

a SECRET or CONFIDENTIAL material originating in another Department or Agency of the Federal Government will not be copied or otherwise reproduced in the Department or Foreign Service without approval of the originator or other individual in the Department or Agency having authority to approve such reproduction, except that Chiefs of Divisions or higher authority may authorize reproduction of such material after consideration of the necessity for reproduction in each instance.

b Distribution outside the reproducing Division of reproduced material originating in another Department or Agency must be specifically authorized in each instance by a responsible officer of the originating agency.

5 REPRODUCTION OF TOP SECRET MATERIAL.

a TOP SECRET material originating in the Department will not be copied or otherwise reproduced in any organizational unit, other than the originating office, without authorization in writing of the Director, or his Deputy, of the Office in which the material originated, or higher authority. At a Foreign Service Post, reproduction of such material must be authorized in writing by the Officer in Charge or the next ranking officer.

b TOP SECRET material originating in a Foreign Service Post will be copied or otherwise reproduced in the Department, if reproduction is essential, only in the Division receiving the material for action, or if the material is of purely informational character, in the Division of the Department receiving the material as a matter of primary interest, except

201.1

V A 5 b (Continued)

that the Chief of the Division receiving such material for action or as a matter of primary interest may, in writing, authorize another Division to reproduce such material provided strict control is maintained over the reproduction process and all copies are strictly accounted for.

c TOP SECRET material originating in another Department or Agency of the Federal Government will not be copied or otherwise reproduced in the Department or Foreign Service without specific approval in each instance of the originator or other responsible individual in the Department or Agency concerned having authority to approve reproduction.

6 COPIES OF TELEGRAMS. The Division of Communications and Records (DC) will reproduce all copies of all telegrams and airgrams required for authorized distribution.

B Marking of Classified Material. When an officer specifies that official material is to have a security classification, the stenographer will indicate on the material the classification and any additional markings required in accordance with the following rules:

1 FORMAL LETTER COMMUNICATIONS. Conspicuously stamp or type the classification in the *upper left corner* and *center bottom* of the first sheet and at the *center top* and *bottom* of each succeeding sheet. When the form permits and the number of copies is small, the classification will be indicated by means of a rubber stamp and colored ink; otherwise, it will be typed in underlined capital letters.

a Office memoranda and other informal communications will have the classification stamped or typed in the *top center* and *bottom center* of each page.

2 TELEGRAMS. The classification assigned a telegram will be conspicuously marked or stamped at the *top* and *bottom* of *each sheet* of the telegram form. Paraphrased copies of classified telegrams also will be stamped or marked with the appropriate classification at the *top* and *bottom* of *each page*.

3 BOOKS AND PAMPHLETS. The classification of books and pamphlets, the pages of which are permanently and securely fastened together, will be shown on the cover, title page, first page, back page, and back cover.

4 MIMEOGRAPHED OR HECTOGRAPHED, MULTILITH AND OZALID REPORTS, DESPATCHES, ETC. Reports, despatches, etc., reproduced in mimeograph or hectograph, multilith and ozalid form and bound with staples will be stamped or marked with the classification on the *center top* and *bottom* of *each page*.

5 CLASSIFIED DRAWINGS OR TRACINGS. Classified drawings or tracings will carry a legend of the proper classification in such a position that it will be reproduced on all copies made therefrom. Whenever practicable, classified photographic negatives will be marked in the same manner. Classified motion picture films will be kept in containers which bear the classification mark to which the contents are entitled, and in addition will state in the title the classification thereof. Classified sound recordings will contain

201.1

V B 5 (Continued)

an opening and closing statement indicating the classification of the recording and will be marked with the appropriate classification in the best manner practicable. If marking of the recording is not practicable, its container will be marked.

6 CONTRACTS FOR THE MANUFACTURE OF CLASSIFIED MATERIAL. Contracts for the manufacture of classified material will be plainly and conspicuously marked or stamped with the proper classification on the *center top* and *bottom of each page*.

7 CLASSIFIED MAPS AND PHOTOMAPS. Classified maps and photomaps will be appropriately marked under the scale and on the *top* and *bottom of each sheet*.

C Additional Marking of Classified Documents

1 DOCUMENTS ISSUED TO AUTHORIZED PRIVATE INDIVIDUALS. Documents containing classified information authorized to be furnished to persons not employed by the Federal Government will, in addition to being marked with the security classification, bear the following notation:

This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, or information of vital interest to the Federal Government and is transmitted for official use only.

2 U. S. OFFICIALS ONLY. Documents so marked will be shown to or viewed by officials of the United States Government only. *Note:* Classified telegrams will not be shown to or viewed by other than U. S. officials except under the conditions specified in paragraph XIII D 2.

3 SPECIAL MARKING OF TOP SECRET AND SECRET DOCUMENTS. All TOP SECRET and SECRET documents will show on the record copy the authority for the classification, the initials of the officer approving the classification and the date affixed. (See Paragraphs IV, A1 and 2.)

4 MARKING FOR LOOSE FILE. The top document or covering paper of a group or file of associated papers will contain an indication of the classification of the highest graded material contained therein. In assembling a file, if any of the under papers have a classification higher than that of the topmost document, a sheet of paper or transmittal slip conspicuously stamped or marked with the classification of the highest classified material contained therein will be used to cover the whole file.

5 SPECIAL MARKINGS FOR TELEGRAMS.

a The words *VERBATIM TEXT* will be placed at the top of the first page of each outgoing telegram containing a verbatim quotation from a note, an agreement, or other document, which has been or is intended to be shown or communicated to officials of foreign governments, the press or similar entities outside the U. S. Government. The notation, *VERBATIM TEXT* will also be used whenever the drafting officer knows that the information in the telegram has been discussed with or is liable to be released in the near future to persons outside the U. S. Government.

201.1

V C 5 (Continued)

b For convenience or economy it may be desirable to transmit in airgram form the text or a portion of the text of a telegram which has been sent or received in encrypted form. When such airgrams are identified with the telegram quoted, they will bear the following notation at the top of the first page:

This airgram contains information taken from an encrypted telegram and must be handled as prescribed for the true reading of such telegrams.

c All true readings or paraphrased versions of classified telegrams communicated to persons outside the Department or the Foreign Service will bear the following notation:

Reproduction of this message in any form is not authorized.

VI RESPONSIBILITY FOR SAFEGUARDING CLASSIFIED MATERIAL.

A The responsibility for the maintenance of the security of classified information rests upon each person having knowledge thereof, no matter how obtained. *impl. by the ss. branch.*

B Public or private discussion of classified information with or in the presence or hearing of any person not authorized to have knowledge thereof is strictly forbidden. This rule is aimed especially at persons inclined to engage in discussions of office affairs with their families or friends outside of the office; it also applies to careless talk in the office in the presence of visitors or workmen, talk in public places, and talk over the telephone involving information classified higher than Restricted.

C **Approval for Public Dissemination.** The inclusion of classified information or material under jurisdiction of the Department or the Foreign Service in any public lecture or course of instruction given or article or book published by an employee of the Department of State or the Foreign Service is strictly prohibited unless specifically authorized by the Secretary of State, one of the Under Secretaries or by the Committee on Unofficial Publication (See Departmental Regulation 183.3, effective 1-1-46.)

1 The above regulation does not preclude the appearance of employees of the Department or Foreign Service before audiences in government operated schools or in official training or indoctrination programs after appropriate clearance has been given of the classified information or material involved.

2 The regulation stated in paragraph VI C above is in addition to and is not to be construed as being in conflict with the provisions of Departmental Regulation 234.3, "Information Issued to the Public" (effective 1-1-46); Departmental Regulation 234-c, "Public Appearances by Department Officers" (effective 2-13-46); and Departmental Regulation 393-b, "Limitation on Activities of Officers of the Department of State and of the Foreign Service in Connection with Programs and Activities of Private Organizations" (effective 6-21-45).

201.1

VI (Continued)

D **Unauthorized Publication or Dissemination.** The unauthorized publication or other unauthorized dissemination of classified material of the Department or Foreign Service is prohibited by law. Section 135, title 22 of the United States Code provides as follows:

Whoever, by virtue of his employment by the United States, shall obtain from another or shall have custody of or access to, or shall have had custody of or access to, any official diplomatic code or any matter prepared in any such code, and shall willfully, without authorization or competent authority, publish or furnish to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

Note: Most classified material in the Department or Foreign Service has been or will have been transmitted in coded form at some time.

E Although material or information having a security classification may not be communicated to the press, the classification of such material or information may be cancelled in accordance with paragraph IV B and Departmental Regulation 201.3, and the information then released to the press through authorized press relations channels, or, in the case of material which must be released for publication abroad, by authority of the Chief of Mission or higher authority.

F **Testimony Before Congress.**

1 When an employee of the Department of State appears before a committee of the Congress and is called upon to give testimony which he knows to be CONFIDENTIAL or RESTRICTED, he will respectfully request that his statements be taken in executive session only and not appear in the record of hearings, the Congressional Record, or other documents open to public inspection.

2 When called upon to give testimony which he knows to be TOP SECRET or SECRET, unless he has previously been authorized by the Secretary of State to give such testimony, he will respectfully state that he is not authorized to disclose the information desired, and will inform the appropriate Member of Congress that a written request for the specific information should be transmitted to the Secretary of State. Testimony of a TOP SECRET or SECRET nature, when authorized by the Secretary of State, will be given only in executive session under the conditions cited in paragraph 1 above.

G **Instruction of Newly Assigned Personnel.** Upon assignment of new officers or clerical personnel who have any part in the preparation, handling, or transmission of classified material, it is the responsibility of the Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities to ensure that such newly assigned personnel receive adequate instruction in the security regulations and procedures of the Department and Foreign Service.

H **Separation of Personnel From Department or Foreign Service.** Personnel leaving the Department or Foreign Service are not authorized, upon separation therefrom, to communicate to anyone information of a classified nature obtained while in the employ of the Department or Foreign Service. Prior to obtaining

201.1

VI H (Continued)

clearance for final salary payment, each employee being separated from the Department will turn in all classified material, identification passes, and keys issued to him while in the employ of the Department. A statement will be obtained from each employee prior to his separation from the Department that none of such material or equipment remains in his possession. Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities will be responsible for instructing personnel leaving the Department or Foreign Service in respect to the above.

VII DISSEMINATION AND DISTRIBUTION OF CLASSIFIED MATERIAL.

A Knowledge or Possession of Classified Matter. No person is entitled solely by virtue of his grade or position to knowledge or possession of classified material. Such material will be entrusted only to those individuals whose official duties require such knowledge or possession.

B Distribution of Classified Information Within the Department and Foreign Service. Distribution of classified material to persons within the Department of State and the Foreign Service will be made on the basis of their functional requirements for such information. Requirements for such information will be determined by the Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service Posts, or by higher authority on the basis of the relationship of persons concerned to a specific undertaking or to general background requirements. The intelligent enforcement of the above-mentioned rule is dependent upon the understanding and collaboration of all responsible officers. In order to facilitate the attainment of the desired objectives, the following procedures are established:

1 Within the Department, the Chief of the Division of Communications and Records (DC) will be responsible, after having been notified of the functional requirements of the various offices and after consultation with the appropriate Chiefs of Divisions, Directors of Offices and higher authorities, for assuring that incoming telegrams, airgrams, despatches, reports, and other materials are properly distributed to organizational units on the basis of organizational functions as defined by Departmental Regulations. Similar responsibilities for the distribution of classified material will be discharged by appropriate officers in the various field offices of the Foreign Service.

2 The Administrative or Executive Officers of the originating or action Division, Office, or Foreign Service establishment, after consultation with their respective chiefs and after consideration of requests from other offices, will be responsible for assuring that there is proper distribution, both within their own offices and to other offices, of all material which originates with their organizations or coming under their jurisdiction for action in the Department or the Foreign Service, and in departmental committees and inter-Departmental committees on which the Department of State is represented. Only established channels of distribution will be utilized.

3 Any disagreement as to the right of an office or person of the Department to receive certain classified information will be referred, in the first instance, to the Directors of Offices or Staff Officers concerned, for direct consideration. If a satisfactory arrangement is not achieved through

201.1

VII B 3 (Continued)

such consultations, the disagreement will be referred through proper channels to the officer of the lowest level having common jurisdiction over *both* disputants or to the Assistant Secretary for Administration or his Deputy, if it is at the staff level. Disagreements in a single establishment of the Foreign Service abroad will be resolved by the Officer in Charge directly concerned.

C Special Rules for Dissemination of Top Secret Material.

1 TOP SECRET material and information will receive the absolute minimum dissemination within the Department and the Foreign Service. It is exclusively for the official use of officers who deal directly with the subject matter and of other persons who have been specifically designated by those officers to work with such material and information. TOP SECRET material and information will be disseminated outside the Department and the Foreign Service only to officers of Federal Departments and Agencies who are known to be qualified to receive it.

2 Each individual of the Department or Foreign Service whose duties require that he work on or have access to TOP SECRET material will first be certified by the Security Officer of the Department for access to such material. A list of personnel in the Department for which certification to handle TOP SECRET material is desired will be furnished to the Security Officer of the Department by Administrative or Executive Officers of Divisions, Offices and higher levels. A list of personnel in each Foreign Service establishment authorized by the Officer in Charge to handle TOP SECRET material will be maintained by the Security Officer of the Mission and a copy thereof furnished to the Security Officer of the Department for certification.

3 A record will be made on each TOP SECRET document of all persons who have had access to it or have read it.

D Dissemination of Classified Material Outside the Department.

1 Copies or paraphrases of classified material which have originated in the Department or Foreign Service will not be sent to other Federal departments or agencies, or to designated individuals therein, except by an officially signed or initialed transmitting communication or through the official liaison Divisions of the Department whose specific duty it is to make formal distribution and keep records of the material distributed.

2 Classified material originating in another Department or Agency and furnished to the Department of State will not be communicated to a third Department or Agency without the consent of the originating Agency.

3 All requests from private individuals, firms, corporations, or state or municipal agencies for classified information or material of the Department must be addressed to the Department in written form before they will be acted upon. Such requests will be forwarded to the Security Officer of the Department for a review of the security considerations involved when TOP SECRET, SECRET, or CONFIDENTIAL material or information is involved, or when there is any doubt as to the qualification of the person or agency to receive

201.1

VII D 3 (Continued)

RESTRICTED material or information requested or when the need therefor is not clearly justified. Releases of material or information classified higher than RESTRICTED will be made *only for the most compelling reasons*.

a Material or information classified RESTRICTED may be made available to private individuals, firms, corporations, or state or municipal agencies provided *all* of the following conditions apply:

(1) A request in writing has been submitted by the requesting agency for each document or item of information desired. Such requests must state the reason the material is desired and the intended use thereof.

(2) Release of the material or information is clearly advantageous to the Department and is in the national interest.

(3) Department of State or U. S. Government policy on release to the public will not be violated by release of the requested material or information.

b Each request for RESTRICTED material or information of the Department will be submitted to the Division of Public Liaison (PL) who will forward it to the Chief of the originating or action Division and, when appropriate, to the Security Officer of the Department for the purpose of determining whether the material or information involved can be declassified and released or whether release can be made in *classified* form.

c Each request for material or information classified *higher* than RESTRICTED will be submitted to the Division of Public Liaison (PL) who will forward it to the Chief of the originating or action Division and to the Security Officer of the Department *in turn* for the purpose of determining whether the material requested can be declassified and released, or whether it can be released in *classified* form. Release of such material *will not be made* without the concurrence of *both* the Chief of the originating Division *and* the Security Officer of the Department.

d Each request for use of Departmental records by persons who are not officials of the United States Government will be referred to the Division of Historical Policy Research (RE) who will act on such requests in accordance with the principles outlined in sub-paragraphs a, b and c above and in accordance with Departmental Regulation 420.1 and other pertinent regulations.

4 When classified material is disseminated under the provisions of these regulations to persons not employed by the Federal Government, they will be informed in the first instance of the proper safeguards required for the handling and storage of the category of material furnished, so that adequate protection may be provided therefor. Official material containing classified information furnished persons not employed by the Federal Government will, in addition to being marked with one of the security classifications, bear the following notation:

This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, or information of vital interest to the Federal Government and is transmitted for official use only.

201.1

VIII HANDLING AND TRANSMISSION OF CLASSIFIED MATERIAL.

A Use of the Telephone.

1 Information classified *higher* than RESTRICTED will not be transmitted by telephone within the Department or to outside agencies. This rule applies also to establishments of the Foreign Service abroad.

2 It is permissible to *make reference* by telephone to material classified higher than RESTRICTED if such references do not, in the course of conversation, reveal the substance of those portions of material under discussion which are classified higher than RESTRICTED. References to file numbers, dates, and subject (provided the subject itself is not classified higher than RESTRICTED) may be made over the telephone, but great care must be exercised not to reveal substantive matter classified higher than RESTRICTED.

B Transmission of Classified Material.

1 TOP SECRET.

a TOP SECRET material will be handled and transmitted in accordance with the rules given in paragraph b below. The following precautions will be strictly observed:

(1) The transmission of TOP SECRET information will be effected by direct contact wherever practicable.

(2) It is mandatory that transmission and custody of TOP SECRET material be covered by a receipt system.

(3) Under no circumstances will TOP SECRET material be transmitted by registered mail.

(4) Under no circumstances will TOP SECRET telegrams be transmitted by electrical means in the clear.

b Transmission within the Department or within a Foreign Service Post.

(1) TOP SECRET material will be transmitted between organizational units of the Department or within a Foreign Service Post by hand of officer or other trustworthy personnel who has worked with the material. Within the Department, transmission of TOP SECRET material via the Security Messenger Service also is authorized.

(2) Material forwarded by hand of officer or other trustworthy personnel who has worked with the material will be enclosed in at least one envelop or otherwise effectively covered from view.

(3) Material forwarded via the Department's Security Messenger Service will be enclosed in double sealed envelopes. The *inner envelope* will be clearly and plainly stamped or marked TOP SECRET and addressed to the specific officer for whom it is destined by name, office symbol, room number, and building. The *outer envelope* will be similarly addressed and clearly marked VIA SECURITY MESSENGER SERVICE. No security classification will be marked on the outer envelope.

201.1

VIII B 1 b (Continued)

(4) A receipt (Form DS-406 or other suitable receipt form) will be executed covering the transfer of TOP SECRET material, whether transmitted by hand of officer or clerical personnel or by the Security Messenger Service. If transmitted by the Security Messenger Service, the Receipt Form DS-406 will be attached to the outer envelop. *Note:* The regular messenger service of the Department is not approved for the transmission of TOP SECRET material.

(5) Transmission of TOP SECRET material within the Department by any means other than those described in paragraph b(1) above is not authorized unless specifically approved by the Departmental Security Officer. Transmission of TOP SECRET material within a Foreign Service Post by any means other than those described in paragraph b(1) above is not authorized unless specifically approved by the Security Officer of the Post concerned.

(6) Typewritten material in documents will be protected from direct contact with the inner cover by a cover sheet or, if the documents are folded, by folding inward.

Transmission to a Foreign Service Post.

(1) If review by the Division of Coordination and Review (CR) is necessary prior to dispatch, each separate TOP SECRET letter, memoranda, note, instruction, or other TOP SECRET material will have attached a *single unsealed* opaque envelope addressed to the officer in charge of the Foreign Service Post, or to an individual by name, and marked *TOP SECRET - TO BE OPENED ONLY BY THE OFFICER IN CHARGE* (or the name of an individual authorized to handle TOP SECRET instead of to *THE OFFICER IN CHARGE*). The correspondence will be transmitted to the Chief of the Division of Coordination and Review (CR) in a manner prescribed for transmission of TOP SECRET material within the Department. (See paragraph VIII B 1 b.) A receipt will be executed covering delivery of each piece of TOP SECRET material to the Division of Coordination and Review (CR).

(2) After completion of the review process the Division of Coordination and Review (CR) will transmit, by an authorized means, each TOP SECRET communication involved to the proper section of the Division of Communications and Records (DC) for forwarding by Diplomatic Fouch.

(3) If review by the Division of Coordination and Review (CR) is not necessary, each separate TOP SECRET document will be enclosed in a *single* opaque envelope addressed to the officer in charge of a Foreign Service Post, or to an individual by name, and marked *TOP SECRET - TO BE OPENED ONLY BY THE OFFICER IN CHARGE* (or the name of an individual authorized to handle TOP SECRET instead of *TO THE OFFICER IN CHARGE*). The envelope will be *sealed* and then transmitted to the Facilities Branch, Division

201.1

VIII B 1 c (3) (Continued)

of Communications and Records (DC) in a manner prescribed for transmission of TOP SECRET material within the Department. (See paragraph VIII B 1 b.) A receipt will be executed covering delivery of TOP SECRET material to the Facilities Branch, Division of Communications and Records (DC).

(4) TOP SECRET documentary material will be transmitted to a Foreign Service Post in the custody at all time of a Diplomatic Courier.

d
Post).

Transmission Outside the Department (Not to a Foreign Service

(1) TOP SECRET material to be transmitted to another Government Department or Agency will be enclosed in two sealed envelopes and transmitted by hand of officer or other trustworthy personnel who has worked with the TOP SECRET material involved, or will be transmitted via the Department's Security Messenger Service, by the courier system of other Departments or Agencies concerned (if such means are approved by the Departmental Security Officer) or by other means specifically approved by the Departmental Security Officer.

(2) The inner envelope will be addressed to an individual by name, title and full address and will be marked or stamped *TOP SECRET*. If transmitted by an approved messenger or courier system, other than the Department's Security Messenger Service, a receipt will be attached to the inner envelope to be signed by the addressee and returned to the originator. If transmitted by the Department's Security Messenger Service, the receipt form will be attached to the outer envelop.

(3) The outer envelope will be addressed to the individual showing his name, title and full address. *The outer envelope will not bear a security classification marking.*

(4) Correspondence sent through the Division of Coordination and Review (CR) will have attached the correct number of properly addressed envelopes, the inner one marked with the security classification.

(5) The receipt attached to an envelope, whether inner or outer, will be signed by the individual to whom the envelope is addressed, or by a responsible liaison officer, a TOP SECRET control officer, or other person known to be specifically designated to receive such material for the Department or Agency.

Receipt of TOP SECRET Material.

(1) Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service Posts, and higher authorities will appoint certain officers in their offices to be known as TOP SECRET Control Officers, with such assistants as necessary, who will

201.1

VIII B 1 e (1) (Continued)

receive and maintain a register of all TOP SECRET material coming to their respective organizations, and who will be responsible for exercising control over such material while it is in their office.

(2) TOP SECRET Control Officers will open and deliver TOP SECRET correspondence to such individuals as must see and work on the correspondence. Persons who work on TOP SECRET material will be kept to a minimum and will be individually warned against disclosing such matters to personnel whose duties do not require it. In addition, prior to permitting personnel to have access to TOP SECRET material, they will be certified by the Security Officer of the Department.

2 SECRET.

a Transmission within the Department or within a Foreign Service Post.

(1) Between buildings and between Divisions of different Offices located in the same building, SECRET material will be transmitted by hand of officer or other responsible personnel, or through the *regular* Messenger System of the Department. Transfer of SECRET material in such cases will be covered by receipt. If transmitted via the regular Messenger Service of the Department, Receipt Form DS-406 will be used.

(2) Between Divisions of the same Office located in the same building, SECRET material will be transmitted by hand of officer or other responsible personnel or by regular messenger. Transfer of SECRET material in such cases need *not* be covered by a receipt. Control of such material will be maintained by registering it in and out of the offices involved in the transfer of material.

(3) SECRET material forwarded through the Department's regular Messenger System or carried by hand of officer or other responsible personnel will be enclosed in a single sealed envelop. For this purpose, Receipt Form DS-406 will be used wherever practicable. The security classification will not be marked on the envelope in such cases.

(4) Transmission of SECRET material within the territorial jurisdiction of a Foreign Service Post will be accomplished by diplomatic courier, either an officer of a Foreign Service Post or a regularly assigned courier of the Diplomatic Pouch and Mail Service, an officer of the Armed Services or through the courier facilities of the Armed Services. Within and between buildings of a Foreign Service Post a messenger service utilizing U. S. citizens only and approved by the Security Officer of the Post may be used. Transfers by such means will be covered by receipts.

201.1

VIII B 2 a (Continued)

(5) Telegrams, airgrams, despatches, and other similar SECRET material which are *regularly* distributed from a central distribution point, where a record of distribution is kept, will be covered by a receipt, one receipt covering the entire contents of a single envelope. Office Message Centers and other subdistribution points, will obtain receipts for SECRET material distributed to other than their own Divisions located in the same building in which the Office Message Center is located.

(6) Transfers within the Department of SECRET material received from other Departments or Agencies of the Government will be covered by receipt in each instance of a transfer within the Department of State.

(7) Typewritten material in documents will be protected from direct contact with the inner cover by a cover sheet or, if the documents are folded, by folding inward.

(8) The envelope enclosing SECRET material will be opaque and will be addressed by name, office symbol, room number and building. No classification stamp or mark will be used on the envelope to indicate its SECRET contents.

(9) Within the Department, receipts attached to envelopes containing SECRET material will be signed by the addressees and returned through the regular Messenger System to the senders.

Transmission to a Foreign Service Post.

(1) If review by the Division of Coordination and Review (CR) is necessary prior to dispatch SECRET letters, memoranda, notes, instructions, or other SECRET material will have attached single *unsealed* opaque envelopes addressed to the officer in charge of the Foreign Service Post, or to an individual by name, and will be marked *SECRET*. Such material will be transmitted to the Division of Coordination and Review (CR) in a manner prescribed for transmission of SECRET material within the Department. Receipts will be executed covering delivery of the SECRET material to the Division of Coordination and Review (CR).

(2) After completion of the review process, the Division of Coordination and Review (CR) will transmit, by an authorized means, the SECRET communications involved to the proper section of the Division of Communications and Records (DC) for forwarding by Diplomatic Pouch.

(3) If not cleared through the Division of Coordination and Review (CR), SECRET material will be enclosed in a single *sealed* envelop, completely addressed, and stamped *SECRET*, and the

201.1

VIII B 2 b (3) (Continued)

envelop will be transmitted by an approved means to the Facilities Branch of the Division of Communications and Records (DC) for forwarding via Diplomatic pouch facilities. Receipts will be executed covering delivery of such SECRET material to the Facilities Branch of DC.

(4) SECRET material will be transmitted to a Foreign Service Post under custody at all times of a Courier designated by the Diplomatic Courier Service.

c
Post).

Transmission Outside of the Department (not to a Foreign Service

(1) SECRET material, other than cryptographic material (see paragraph XIII F 3) to be transmitted outside the Department, except to Foreign Service Posts, will be enclosed in two sealed envelopes and transmitted by hand of officer or other responsible personnel, by the messenger system of the Department or Agency to which the material is addressed (if such transmission means is approved by the Departmental Security Officer) or by United States Registered Mail with return receipt requested.

(2) Both envelopes will be properly and completely addressed, and the inner one marked SECRET. The outer envelope will not be stamped or marked with the security classification.

(3) A receipt will be attached to the inner envelope for signature of the addressee and return to the sender.

3 CONFIDENTIAL. CONFIDENTIAL material will be prepared and transmitted in accordance with the following rules:

a
Post.

Transmission within the Department or within a Foreign Service

(1) CONFIDENTIAL material will be prepared and transmitted within the Department or within a Foreign Service Post by hand of officer, responsible clerical personnel, or through the regular messenger system, if such means is approved for handling CONFIDENTIAL material by the appropriate Security Officer (the Departmental Security Officer in the case of material transmitted within the Department or the Security Officer of the Foreign Service Post concerned in the case of material transmitted within a Foreign Service Post).

(2) The regular messenger service of the Department is authorized for transmission of CONFIDENTIAL material.

(3) Transmission of CONFIDENTIAL material need not be covered by a receipt unless deemed necessary by the sender in cases of unusual importance.

201.1

VIII B 3 a (Continued)

(4) CONFIDENTIAL material will be prepared for transmission in double sealed envelopes except when transmitted via hand of officer, responsible clerical personnel, or the regular Messenger System of the Department, in which case a single envelop will be used. When double envelopes are used, both will be addressed with the name, room number and building of the addressee and the inner envelop will be stamped or marked CONFIDENTIAL. The outer envelop will not be marked with the security classification. When transmitted via the Department's regular Messenger System the single envelop used will be opaque and will contain the name, room number, and building of the addressee. No security classification will be indicated thereon.

b Transmission to a Foreign Service Post.

(1) CONFIDENTIAL material will be transmitted to Foreign Service Posts by Diplomatic Fouch facilities.

(2) CONFIDENTIAL material for transmission via Diplomatic Fouch facilities will be forwarded to the Facilities Branch, Division of Communications and Records (DC) by a means authorized for transmission of CONFIDENTIAL material within the Department or, if such material must be reviewed by the Division of Coordination and Review (CR), it will be transmitted to CR via an authorized means, and CR will accomplish transmission to the Facilities Branch of the Division of Communications and Records (DC).

(3) If the material is reviewed by the Division of Coordination and Review (CR), a completely addressed, unsealed envelop, marked or stamped CONFIDENTIAL will be attached to the file.

(4) If not reviewed by the Division of Coordination and Review (CR), the material will be enclosed in a sealed envelope, bearing the complete address of the individual in the Foreign Service Post for whom the communication is destined, and will be stamped or marked CONFIDENTIAL. Transmission to the Facilities Branch, Division of Communications and Records (DC) will be accomplished in a manner approved for transmission of CONFIDENTIAL material within the Department.

c
Post).

Transmission Outside of the Department (Not to a Foreign Service

(1) CONFIDENTIAL material to be transmitted outside of the Department will be enclosed in double sealed envelopes and transmitted by hand of officer or other responsible personnel, by the regular Messenger System of the Department or Agency to which the material is addressed, (if approved by the Departmental Security Officer), or by United States Registered Mail with return receipt requested.

(2) Both the inner and outer envelopes will be completely addressed. The inner envelope will be stamped or marked CONFIDENTIAL. The outer envelope will not be marked with the security classification.

201.1

VIII B 3 c (Continued)

(3) Transmission of CONFIDENTIAL material need not be covered by a receipt unless the sender considers the material involved of unusual importance.

4 RESTRICTED. RESTRICTED material will be prepared for transmission in a single opaque envelope bearing no security classification.

a Within the Department. RESTRICTED material will be transmitted within the Department through the regular Messenger System of the Department or by hand of responsible person.

b To a Foreign Service Post. RESTRICTED material will be transmitted by Diplomatic pouch facilities. RESTRICTED material will be sent to the Facilities Branch, Division of Communications and Records (DC) in a manner prescribed for transmission of RESTRICTED material within the Department. If it is necessary for the Division of Coordination and Review (CR) to review the material, it will be sent through CR.

c Outside the Department (Not to a Foreign Service Post). RESTRICTED material may be transmitted outside of the Department by the regular mail and messenger service of the Department, by the messenger service of other Departments or Agencies, or by ordinary mail, provided it does not pass through the mail service of any foreign government.

IX CUSTODY AND STORAGE OF CLASSIFIED MATERIAL.

A Custody.

1 Each custodian of classified material will exercise vigilance and initiative in applying the basic rules governing the use, handling and storage of classified material.

2 When an officer delegates authority to personnel under him to handle and have custody of TOP SECRET, SECRET, CONFIDENTIAL or RESTRICTED material, he will not consider himself relieved of the responsibility of insuring that the material so entrusted is properly safeguarded.

B Storage. The term *storage* as here used, refers to the physical or mechanical means or other security measures taken to protect classified material outside of working hours, or to the manner in which it is protected during working hours when not under the personal supervision of the individual to whom it was issued.

1 Within the Department, TOP SECRET material will be stored in vaults, safes, or steel safe-file cabinets equipped with three-combination lock or will be under protection of a means specifically approved by the Security Officer of the Department.

2 Within the Department, SECRET material will be stored in a manner authorized for TOP SECRET material or in steel file cabinets equipped with a steel bar and lock set, or in steel file cabinets equipped with plunger-type

201.1

IX B 2 (Continued)

lock and supplemented with *wonder* locks, provided the keys to locks of such files are stored behind a three-combination lock and carefully accounted for to insure against unauthorized duplication. Other means for storing SECRET material must be authorized specifically by the Departmental Security Officer.

3 Within the Department, CONFIDENTIAL material will be stored in a manner authorized for the storage of TOP SECRET or SECRET material, in metal file cabinets equipped with *either* plunger type or *wonder* locks, or in a manner specifically authorized by the Departmental Security Officer.

4 Both within the Department and the Foreign Service RESTRICTED material will be stored in the best practicable manner insuring a reasonable degree of security. A reasonable degree of security is defined to mean protection from easy access or view by persons outside of the government. Authorized containers for RESTRICTED material include file cabinets, desks, bookcases, supply cabinets, or other containers located in a building, protected by building guards. In buildings not protected by building guards, RESTRICTED material will be stored out of sight in a locked room or in a locked container.

5 At Foreign Service Posts TOP SECRET material will be stored in vaults, safes, or steel file cabinets equipped with three-combination lock. SECRET, and CONFIDENTIAL material will be stored in vaults, safes, or steel file cabinets equipped with three-combination lock or in steel file cabinets equipped with *bar and lock set* with American made locks or by other means, approved by the Security Officer of the Post concerned, which affords equivalent security.

6 Where steel file cabinets equipped with plunger type locks are used, care will be exercised to insure that all drawers are properly caught when closed and that drawers cannot be opened by applying pressure upon them in any direction when the cabinets are locked. Where *wonder* locks are used, care will be exercised to insure that drawers are closed in such a manner as to be level with the front of the file cabinets and that *wonder* locks are pushed forward on their supporting bars as far as possible.

7 Keys to plunger type, *wonder*, and other types of key locks (except door locks) will be stored behind a three-combination lock. They *will not* be carried on the persons of individuals. Any duplication of keys required will be made *only* by the Security Officer at Division, Office, FS Post, or higher levels. A report will be made to the Department Security Officer of all such keys duplicated. Keys to doors will be left in custody of building guards after working hours.

8 The name, address, and telephone number of each person knowing the combination of a safe or safe file will be entered on a list pasted on the outside front of the safe or safe file cabinet. A similar list of personnel responsible for locking file cabinets equipped with plunger-type or *wonder* locks or padlocks will be posted on the outside front of the file cabinets.

9 The combination of each safe will be changed at least once a year, and at such other times as necessary (as when any person knowing the combination severs his connection with the office in which the safe is located).

201.1

IX B 9 (Continued)

Combinations of all safes and safe-files in their respective areas will be handled as SECRET information and will be kept on file by the Security Officers of Divisions, Offices, Foreign Service establishments, and higher authorities. A duplicate copy of the combinations of all Departmental safes will also be filed in the office of the Security Officer of the Department.

10 If a safe or file cabinet is found unlocked by a building guard during his evening inspections, he will immediately telephone the first person whose name is posted on the safe or file cabinet, or other persons listed, and guard the safe or cabinet until the individual concerned reports to the office and inspects the unlocked safe or file cabinet to determine if any material is missing. Classified material found outside a storage place by the guards or other inspectors will be locked in the most conveniently located place possessing adequate security or placed under guard until delivered to the Departmental Security Officer. A report of unlocked safes or file cabinets or classified material not properly stored and of the action taken by the building guards will be made to the Security Officer of the Department on the morning following the occurrence.

C Removal of Official Material from the Department.

1 TOP SECRET. No officer or employee of the Department of State will take TOP SECRET material from the Department except for the conduct of official business. Under no circumstances will TOP SECRET material be removed from the Department outside of working hours except where official conferences or consultations are involved. Specific approval *in writing* by Directors of Offices or higher authorities will be given for such use of TOP SECRET material and copy of the authorization for removal will be filed by the TOP SECRET Control Officer of the office concerned. The date of return of the material to the office concerned will be entered upon the written authorization for removal which is held by the TOP SECRET Control Officer.

2 SECRET AND CONFIDENTIAL.

a Normally SECRET and CONFIDENTIAL material will not be removed from the Department for purposes of working with it outside of office hours. However, in case of necessity an officer may remove SECRET or CONFIDENTIAL material from his office for such purpose if permission has been granted by the Chiefs, or their deputies, of Divisions or higher levels. For such cases, there will be maintained in the office of the approving authority, a permanent registry record of the material removed, describing the material, and giving the date of removal, the name of the officer removing the material, the name of the officer authorizing removal and the date of return. The officer removing material will certify that he will assume responsibility for protecting the material in a manner commensurate with its classification.

b An inspection of such registers will be made regularly by the Security Officer of the Department.

3 RESTRICTED. Material classified RESTRICTED (except copies of classified telegrams bearing the notation "paraphrase before communicating*****", which will be handled as prescribed for SECRET) may be removed from the Department outside of regular office hours provided means are available to insure a reasonable degree of security for the material.

201.1

IX C (Continued)

4 Classified material removed from the Department will not be read or revealed in a public place.

5 Any material removed from the Department will be returned as soon as practicable to its proper place within the Department.

D Action on Resignations.

1 When an employee resigns, or otherwise severs his connection with the Department of State or Foreign Service, all classified material in his custody, his identification pass, and all Departmental keys in his custody will be turned in to the Department. Classified material which must be turned in includes personal files and any other types of material which contain classified information. Prior to giving final clearance for an employee to receive his termination pay, his immediate supervisor will be responsible for insuring that all classified material, identification passes and keys, in custody of the employee concerned have been turned in.

X OFFICE SECURITY.

A Designation of Officers to Enforce Security Measures. The Chiefs of Divisions, Directors of Offices, Officers in Charge of Foreign Service establishments, and higher authorities will designate a person in their respective organizational units (normally the Executive or Administrative Officer) to be responsible for enforcing security measures within their respective offices. In large offices, where it is not possible for one person to maintain effective supervision over all classified material, an additional employee or employees will be designated (to be known as Assistant Division, Office, or Mission Security Officers) in each room or group of rooms to assist in seeing that all classified material is properly handled during the day and properly stored when the office is closed. Designating additional employees as Security Officers and Assistant Security Officers will not relieve the Division Chief, Office Director, Officers in Charge of Foreign Service establishments, or higher authority of the responsibility of insuring that all material entrusted to the organizational unit under his jurisdiction is properly safeguarded.

B Handling Classified Material During Working Hours.

1 TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED material will not be left on desks or otherwise exposed in an unoccupied office. When it is necessary to leave an unoccupied office, classified material will be stored as indicated in paragraph IX B.

2 INSPECTION BY UNAUTHORIZED PERSONS. Employees using classified material will take every precaution to prevent deliberate or casual inspection of it by unauthorized persons. One effective precautionary measure is to keep the papers face down or covered when not in use directly; another is to have a conference table located near the entrance to the office where the officer can interview visitors. These and other such practices will provide safeguards against the possibility of unauthorized persons seeing classified material. Only those persons who must handle the material for processing or appropriate action will be permitted to see it.

201.1

X B (Continued)

3 CARBON COPIES, STENOGRAPHIC NOTES, ETC. All the rules prescribed herein for safeguarding other classified material will apply also to such items as copies of classified official documents and any informal materials, such as memoranda, rough drafts and shorthand notes, carbons and carbon copies, which contain classified information.

4 Within the Department, a report will be made to the Departmental Security Officer, through the appropriate Division, Office, or higher level Security Officers, of improper security preparation, safeguarding or transmission of classified documents. A similar report will be made to Foreign Service establishment Security Officers by employees of Foreign Service establishments.

5 A registry system will be established in organization units of Divisions, Offices, Foreign Service establishments, and higher level offices, to control effectively TOP SECRET, SECRET, and CONFIDENTIAL material processed by those organizational units.

6 Classified material will not be delivered to desks in unoccupied rooms. At the close of working hours, all document baskets will be carefully checked to insure that deliveries of classified material have not been made to desks of absent personnel.

7 A security plan will be devised by the Security Officers of organizational units to insure that proper security measures are observed during office moves. Such security plan will include provisions for assuring that containers of classified material are securely locked, clearly and distinctly addressed, and a means provided for accounting for their dispatch and receipt by responsible persons. While in transit, they will be accompanied by responsible persons.

8 Carbon paper, which has been used in typing hectograph sheets, mimeograph stencils, and tissue sheet copies of classified material, will be handled and stored in a manner commensurate with the security classification of the original of the material involved.

C Safeguarding Classified Material After Working Hours. All classified material will be removed from desks and trays and placed in storage for the night in accordance with the storage rules prescribed in Paragraph IX B. The Security Officers of Divisions, Offices, Foreign Service establishments, or higher levels will cause to be instituted a system of security checks at the close of each working day to insure that the persons responsible for classified material are properly carrying out their duties and to check on the locking of safes and file cabinets.

XI DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL.

A Destruction of Classified Material. The general rule for the destruction of all classified material is that it will be carefully and completely burned in the presence of responsible persons. Disposable classified material comprises information copies of telegrams and airgrams, memoranda, extra copies, rough drafts, shorthand notes, carbon papers, and any other non-record material which contains classified information.

201.1

XI A (Continued)

CAUTION: Classified *record* copies of official material will *not* be burned or otherwise destroyed. Classified material will *not* be deposited in ordinary wastebaskets.

B Destruction Procedure in the Department.

1 All classified waste material to be disposed of will be torn into small pieces and placed in paper containers designated as *burn-bags*. Outside of regular working hours partially filled burn-bags will be stored in a manner affording protection commensurate with the classification of material to be burned (see paragraph IX B). Burn-bags will be sealed by stapling when filled and clearly and distinctly marked *Burn*.

2 Responsible persons within each Division, Office or higher level office will be designated to deliver filled burn-bags to designated custodians at one of the collection points listed in Departmental Regulation 201.2 in accordance with the collection schedule indicated therein.

3 a Responsible employees of the Division of Central Services (CS) have been designated to collect the filled burn-bags at the locations designated. Until completely burned in the presence of a responsible person all such material will be protected by security safeguards commensurate with the classification of material involved.

b Except for classified material originated by the destroying officer, a record of material destroyed will be maintained in the office in which TOP SECRET, SECRET, and CONFIDENTIAL material is torn up and placed in *burn-bags*. The Chief of each Division, Office, and higher level office will be responsible for establishing such a record of destruction suitable to his operation and one which will enable responsibility to be fixed in cases of wrongful destruction. The Security Officer of the Department will, upon request, assist in devising a procedure for recording destruction of TOP SECRET, SECRET, and CONFIDENTIAL material in organizational units of the Department. From time to time the Security Officer will inspect records of classified material destroyed in organizational units.

C Destruction Procedure at Foreign Service Posts. The procedure to be followed at Foreign Service Posts for destroying classified material will be prescribed by the Security Officer of the Post concerned and will be in accordance with the principles outlined in paragraphs XI A and B above. Persons witnessing the destruction of classified material must be United States citizen employees. A record of TOP SECRET, SECRET, and CONFIDENTIAL material destroyed will be maintained at each Foreign Service Post. Such records will be inspected periodically by the Security Officer at each Post.

XII DEPARTMENTAL BUILDING SECURITY.

A Since pass control systems are not in general operation to restrict entrance into State Department Buildings during working hours, extreme care must be exercised by all officers and employees handling classified material during the day. Such material will be safeguarded at all times as prescribed in paragraph X B above, which prescribes regulations for handling classified material during working hours.

201.1

XII (Continued)

B Pass controls are in operation after working hours and employees are required to present identification passes to the guards and to sign a register when entering or leaving any Department of State building outside of regular working hours. Employees who do not voluntarily present identification passes to guards after working hours will be specifically requested by the guards to show their passes.

C Visitors will not be permitted in any Department of State building after working hours, unless they are escorted in and out of the building by an employee from the office of the person on whom they are calling or unless the building guard is authorized to admit the visitor by the person on whom the visitor is calling.

D All keys of office doors kept locked after working hours will be turned in to the building guards to be held in their custody after working hours.

XIII CRYPTOGRAPHIC SECURITY. The following regulations, in addition to those prescribed in Sections I through XII above, are concerned with the safeguarding of cryptographic material and are designed to assure a high degree of cryptographic security in the Department and the Foreign Service.

A Drafting Classified Telegrams.

1 Each telegram will be drafted to be as brief as is consistent with clarity and completeness.

2 Punctuation will be held to a minimum. Prepositions, pronouns, parts of the verb *to be*, and articles (particularly *the*) will be omitted where possible. Recognized or authorized abbreviations may be substituted for the complete words where they would be readily understood by officers of the Department and the Foreign Service. In referring to previous telegrams, the hour designation is necessary only to identify circular telegrams.

3 Set forms of expression and repetitious phraseology will be avoided in drafting telegrams with similar texts to prevent the compromise of a cryptographic system through similarities in the resulting encrypted texts. The necessity for repeating the same basic text with only minor changes in each telegram can often be avoided by including the information for all addressees in one multiple-address telegram, or by substituting words such as *the country to which you are accredited* for individual names. In other cases one telegram may be repeated to all addressees containing the identical information and a separate telegram may be sent to each addressee with the different information. If other methods are not applicable, paraphrasing will be employed to vary the phraseology of telegrams which would otherwise be drafted with long identically worded passages.

4 Words and expressions commonly used will be avoided at the beginnings and endings of telegrams. A deliberate attempt should be made to conceal in the text a direct reference to a previous communication, an internal address or signature, and routing or delivery instructions. Commonly used words which should not appear as the first word of a telegram are: Dept., Embassy, Legation, Please, and Following. Commonly used last words to be avoided are: advise(d), follow(s), informed, urgently, and (un)quote. The first or last word of a telegram should not be the name or nationality of the country or place to which the telegram is addressed or from which it is sent.

201.1

XIII A (Continued)

5 Two separately numbered telegrams will be sent in preference to one long telegram involving only a small amount of classified information. The classified telegram may refer to the plain language telegram, but the reverse is never permissible.

6 Whenever the drafting officer knows that the information in a classified telegram has been or may be communicated to persons other than American employees of the U. S. Government he will indicate this fact or possibility by the marking VERBATIM TEXT at the top of the telegram as explained in paragraph V C 5 a.

7 Originators of classified telegrams in the Department will prepare only the number of copies desired by the Division of Communications and Records (DC), plus one copy for retention until a confirmation copy is received from the Division of Communications and Records (DC).

B Classification of Telegrams.

1 The Officer drafting a telegram is responsible for indicating its correct security classification.

2 The classification of each telegram must be given careful consideration since over-classification and under-classification are equally to be avoided.

3 Each telegram making a direct reference by subject matter or other identifying information to a telegram classified CONFIDENTIAL or higher will be classified at least CONFIDENTIAL. Each telegram making a direct reference to a telegram classified RESTRICTED will be classified at least RESTRICTED. An UNCLASSIFIED telegram will not contain a direct reference to a classified telegram.

4 The security classification will be clearly indicated on the top and bottom of the hectograph copy prepared and on each sheet or copies thereof. If classified TOP SECRET, the abbreviation TOPSEC will also be placed in the text near the beginning.

C Transmission of Classified Telegrams.

1 True readings of classified telegrams will be distributed within an establishment only by the Message Center. When it is desired that other offices receive information copies of such telegrams the Message Center (Code Room) will be notified and copies forwarded through normal channels.

2 The serial identification number, as well as any serial numbers used within the text as references to other classified telegrams, will be deleted before a classified telegram is communicated to any one outside the United States Government service. Every possible effort will be made to disguise the fact that the text communicated was taken from a telegram.

3 If it is essential that the contents of a classified telegram be transmitted by mail or messenger to another establishment in true reading form, it will be transmitted with the safeguards applying to SECRET material, unless

201.1

XIII C 3 (Continued)

it is TOP SECRET, in which case it will be transmitted with the safeguards applying to TOP SECRET material. (see also paragraphs V C, 5 b and c).

4 The transmission to another establishment by mail or messenger of copies of the plain text of encrypted telegrams for confirmation purposes is strictly prohibited.

D Paraphrasing.

1 Paraphrasing is employed as a protective measure for certain cryptographic systems.

2 The text of a telegram will be carefully paraphrased when the copy distributed is marked "Paraphrase Before Communicating*****" and the information therein is to be communicated to persons other than American employees of the U. S. Government. The paraphrased version transmitted will not show the serial number of the original telegram or the serial numbers of any classified telegrams used as references within the text.

3 When paraphrasing is employed all of the following processes will be applied to the text of the message:

a Change the order of the paragraphs.

b Alter the position of the sentences in each paragraph.

c Shift the positions of the subject, predicate and modifiers in each sentence.

d Substitute synonyms or equivalent expressions, but exercise care to assure that confusion of meaning does not result.

e If the above-mentioned steps have not changed the length of the paraphrased version try to use other phrases, clauses, and synonyms in order that the paraphrased text will vary at least 15 per cent from the original text.

E Use of Cryptographic Systems.

1 No cryptographic system will be used unless it has been issued or approved by the Chief of the Division of Cryptography (CY) of the Department.

2 The number of persons allowed to have knowledge of the Department's cryptographic systems will be limited to those requiring such information for the performance of their duties.

3 The following persons are authorized to see and make use of cryptographic material when their duties require a knowledge of cryptographic operations; commissioned officers of the Foreign Service and specifically designated employees of Missions approved by the Chief of the Division of Cryptography (CY) and the Security Officer of the Department; specifically designated employees of the Division of Communications and Records (DC); employees of the Division of Cryptography (CY); and the Security officer of the Department and of each Foreign Service Post.

201.1

XIII E (Continued)

4 Only United States citizens will be authorized by the Security Officer of the Department to perform cryptographic work and have access to the Department's cryptographic systems.

5 No one will be permitted to encrypt messages for transmission until he is thoroughly familiar with security regulations in general, the Cryptographer's Manual, and the detailed instructions provided for the operation of the cryptographic systems concerned.

6 A clerk recruited locally at a Foreign Service Post will not be assigned to cryptographic duties until he has served at that post for at least six months, and approval of the Department obtained or indicated in paragraph 3 above.

F Special Rules for Safeguarding Cryptographic Material.

1 Careful consideration will be given to the location and arrangement of code rooms and openings thereto in order to prevent the viewing of exposed cryptographic material by unauthorized persons. Only those persons whose duties require access to the Code Room will be allowed to enter it. A notice will be prominently displayed on the outside of the door to the Code Room with the following words on it, *RESTRICTED AREA - NO ADMITTANCE*.

2 When it is necessary for unauthorized persons to enter the Code Room, such as for cleaning or building maintenance, all cryptographic operations will be stopped and the cryptographic material will be stored as required for unattended material or it will be covered and guarded.

3 Cryptographic material to be transmitted to or from the field will be securely wrapped in heavy paper, will be sealed or tied, and marked *SECRET*, and the package will then be transmitted via Diplomatic Fouch facilities.

4 Cryptographic material will be stored in a three-combination safe or safe file or in a manner which provides equivalent security and which has been approved by the Departmental Security Officer, or the Security Officer at the Foreign Service establishment concerned.

5 All vaults and safes containing cryptographic material will be locked when the room in which they are located is left unguarded.

6 A destruction plan will be formulated by all custodians of cryptographic material and necessary material will be readily available to effect the complete and total destruction of cryptographic material in the event of an emergency. Destruction plans will include burning, smashing equipment with heavy instruments, and any other action designed to render cryptographic material unrecognizable and insure its complete destruction.

7 On suspicion or evidence that unauthorized persons have obtained possession of or copied elements of a cryptographic system, its use will be discontinued at once and the Department will be notified as to the elements concerned and advised whether the compromise is certain, probable, possible or improbable.

XIII (Continued)

G Responsibility for Cryptographic Security.

1 The Chief of the Division of Cryptography (CY) is the Cryptographic Security Officer for the Department and, in collaboration with the Security Officer of the Department is responsible for the formulation of all cryptographic security rules to be observed in the Department and in the field.

2 The officer personally responsible for the issuance and enforcement of cryptographic security rules at each Foreign Service Post will be known as the Cryptographic Security Officer. Although the Officer in Charge is responsible for cryptographic security, he may designate another officer assigned to the post to act as Cryptographic Security Officer.

3 The Cryptographic Security Officer will be the Custodian of cryptographic material issued to his post. In the Department the Officer in Charge of the Telegraph Branch will be the Custodian of cryptographic material issued for current use by the Telegraph Branch and the Chief of the Division of Cryptography will be the Custodian of all other cryptographic material.

4 A daily check on the status of cryptographic material will be made at each office. Each person in a responsible position where cryptographic material is used under his supervision will maintain a daily record or keep a running inventory of all such material as it is removed from its storage place during each work day or shift. If this record or inventory discloses the loss of any material, a careful search will be started at once and a report of the circumstances will be made forthwith to the Cryptographic Security Officer directly concerned. After investigating and evaluating a loss, the Cryptographic Security Officer will make a report to the Department (Division of Cryptography (CY)).

5 On January 1 and July 1 of each year the Cryptographic Security Officer will cause an inventory of all cryptographic material in his custody to be made by two officers (one officer at posts having only one assigned) and a list of this material by Short Titles and register numbers will be forwarded to the Department, Division of Cryptography (CY). (Foreign Service Form 345).

6 When cryptographic material is destroyed the destruction will be witnessed by two officers (one officer under unusual conditions of necessity - explanation of such conditions will be submitted with the report of destruction) and a report signed by these officers listing the Short Titles and register numbers of this material will be submitted to the Department, Division of Cryptography.

7 When a permanent transfer of officers takes place, the officer assuming charge will submit to the Department, Division of Cryptography, an inventory report listing the Short Titles and register numbers of the cryptographic material on hand. (Foreign Service Form 345).

INDEX TO SECURITY REGULATIONS OF THE DEPARTMENT OF STATE

- A -

Access	
to classified material	VIIA, B, C2, 3; XB2
to Code Room	XIIIF1,2
Accumulated Files	IVB2
Additional safeguards, for transmitting	
Top Secret Material	VIIIB
Address, in classified telegrams	XIIIA4
Addressing, classified material	VIIIB1b (3), c (1), (3), d (2), (3), 2a (8), b (1), (3), c (2), 3a (4), b (4), 3c (2)
Administrative Officers	
as security enforcement officers	XA
keep safe combinations on file	IXB
responsible for controlling distribution	VIIIB2
Airgram	
containing quotations from telegrams	XIIIC3
true reading of	IC12
Airgram Service, unclassified material in	IIA
Approving Officer	IVA
Attaching receipts	VIIIB1b (4), c (3), d (2), e (3), (9), 2c (3)
Authority	
for custody of classified material	IXA
for publication abroad	VIE
to approve security classifications	IVA
to classify	IVA
to declassify or downgrade	IVB2, 3, 4, 5
to downgrade or declassify classified material of foreign nations	IVB3
to give testimony	VIF
to make public classified information	VIC, D, E
Authorization	
for removal of classified material from Department	IX C
to see classified material	VIIA, B, D2
to see Top Secret material	VIIC
to use cryptographic system	XIIIE

- B -

Baskets, document check of	XB6, C
Books, classification of	VB3
Burn Bags, procedures in use for	XIB
classified waste	XIB
Cabinets, for storage of classified material (see also containers, safes)	IXB
Cancelling or changing, classifications	IVB

Carbons, as classified material.	IC1, XB3,8, XIA
Careless talk.	VIB
Certification for access to Top Secret.	VIIIBle(2)
Classified Material	
changing classification of.	IVB
custody	IXA
definition.	IC1
Destruction, disposal	XIB
dissemination and distribution.	VA3, VID, VII
downgrading and declassifying	IIF, IVB
extracts from	IIB
knowledge of.	VIIA
marking of.	VB, C
of defunct Agencies	IVB4
of foreign Agencies	IIG, IVB3
of other Agencies	IIG, IVB4, VA4, VIID2
outside of storage place.	IXB
possession of	VIIA
preparation of.	VA, XB4
protection of	IC14, VI
publication of.	VIC
removal from Dept.	IXC
reproduction of	VA
requests for.	VIIB2, VIID1,3
responsibility for.	VIA, XA, B, C,
return of to Dept.	IXC5
review of assigned classifications.	IWA4
right to receive.	VIIB
safeguards.	XB, C
stencils.	XB8
storage	IC14, IXB, XC
telegrams	XIIIA
tissue sheet copies	XB8
transmission of	VIIIB
Collection Points, for classified waste.	XIB2
Confidential information, material	
definition of and examples.	IIIC
dissemination, distribution	VIIA, B, D, VIIIB3
storage	IXB3
transmission of within Dept.	VIIIB3a
transmission of, within Foreign Service Post.	VIIIB3a
transmission of, outside Dept.	VIIIB3c
transmission to Foreign Service Post	VIIIB3b
Containers, for storage of classified material	IXB, XC, XIB
Control Officer for Top Secret material.	VIIIBle
Copies of classified material.	VA, B, VIID1, XB3,8, XIA, XIIIA7, XIIIB4
Copies, confirmation; of telegrams	XIIIC3
Courier System for transmission of Top Secret.	VIIIBlc(4), d(1)
Cryptographic Materials	
classification of	IIIB1f, C2f
definition.	IC3
destruction	XIIIF6
rules for safeguarding.	XIIIF

Cryptographic Security	
definition	IC4
responsibility for	XIIIG
Cryptographic System	
compromise of	XIIIF7
definition	IC5
protection of	XIIID,F
Custodian	
of classified materials	IXA
of cryptographic materials	XIIIG3
Custody	
of Secret, Confidential, Restricted material	IXA
of keys	IXB7, D
of Top Secret material	VIIIB1a(2)

- D -

Declassifying and Downgrading	IC6,8, IIF, IVB
automatic	IIF
authority to	IVB
foreign material	IVB3
material of Other Agencies	IVA4
procedure	IVB7
Declassification Committee	IVB8
Departmental Security Officer, authority and responsibilities	VIIIB2c(1), 3a(1), IXB2,3,7 XB4, XIB3b, XIIIG1
Destruction, destroying	
of classified material	IA, XI
of cryptographic material	XIIIF6
record of	XIB3b
Disposal	
of classified material	XI
of classified telegrams	XI
of classified waste material	XI
of wastage from reproduction	XI
Dissemination and distribution, of	
classified material	VA3, VIIIB,C
outside the Department	VIID
Top Secret	VIIC
of classified telegrams	XIIIC1

- E -

Executive Officers, security responsibilities of	VIIIB2, IXB7,9, D,X
Extracts, from classified documents	IIB2

- F -

File of documents	
classification of	IId
marking of	VC4
Functions of Security Officers of organizational units	XA

- G -

Grading of official material (see classified material)

- H -

Handling, classified material. VIIC2, IA, VIID4, VIII, XB

- I -

Identification Pass, presentation of XIIB
Initials, on record copy IVA1,2, VIID1, VC3

- K -

Keys
duplication of IXB7
protection of IXB2
storage outside of working hours. IXB7

- L -

Locking doors outside of working hours XIID
Loose File, marking of VC4

- M -

Marking
burn-bags XIB1
classified material VB, C,
cryptographic materials XIIIF3
envelops. VIIIB
loose files VC4
material disseminated to
private entities. VC1
security classification on
cover envelops. VIIIB
"Verbatim Text" on telegrams. VC5
Messages, changing classification of IVB6 (b), (c)
Moves, office; security during XB7

- N -

Notations, on classified material. VB, C, VIID4

- O -

Office Security. X
Other Government Agencies
classified material from. IIG, VIID2, VIIIB2a (6)
declassification, downgrading of
material from IVB4
distribution to VIID1
transmission of classified material to. VIIIB1d, VIIIB2c,
VIIIB3c, VIIIB4c
use of courier (messenger) service of VIIIB1d, VIIIB2c,
VIIIB3c, VIIIB4c
Overclassification IIE

- P -

Pages, marking of.	VB
Pamphlets, marking of.	VB3
Paraphrased Telegrams.	
marking of.	VB2, VC5c
transmission of	VD, VIIIA1
Paraphrasing	IC10, XIIID
of extracts from telegrams.	IIB2, XIIID
of telegrams.	IVB6 (b), (c), VB2, XIIID
rules for	XIIID
Pass Control System.	XII
Personnel	
leaving employment of Department.	VIH, IXD
Security instruction of	VIG
Physical Security, responsibility for.	VIA
Preparation of classified material	V
Publication, security rules for.	VIC, D

- R -

Receipt System	
for Confidential material	VIIIB3
for Secret material	VIIIB2
for Top Secret material	VIIIB1
Record of destruction	XIB3b, c
Record Copies.	IValb, 2b, IVB6a, VC3, XIA
Records, of material distributed	VIID, VIIC3, VIIB2, XB5
References	
to classified material, (including via telephone).	VIIIA2, IIB2
in telegrams.	XIIIA2, 4, 5, XIIIB3
Registered Mail, used for transmitting classified material	VIIIB1a (3), VIIIB2c (1), VIIIB3c (1)
Registry System, for classified material	XB5
Release, of classified material.	VIC, VIID3
Reproduction, security rules for	VA, VB
Responsibility	
for enforcement of security	VIA, X, XA, XIIIG
for material in custody of persons leaving employ of Department.	VIH, IXD
for safeguarding.	VIA, IXA, XC, XIB, XIIG, XIIA
for security of information	VIA
Restricted material, information	
communicated via telephone.	VIIIA
definition and examples	IIID
dissemination, distribution of.	VIIB
in testimony.	VIF1
procedure of classification	IVal3
storage of.	IXB4

telegrams.	XIIIB3
transmission of.	VIIIB4
true reading	IVB6 (c)
Reviewing of classified material.	IIIE1, IVA

- 5 -

Safeguarding	
classified material outside of working hours.	XC
cryptographic materials.	XIII
transmission of classified material.	VIIIB
Safes, storage of classified material in.	XB, XIB1
Secret material	
classification procedure	IVA2, 3
control by registry system	IXC2, XB5
definition and examples.	IIIB
destruction of	XIB
dissemination, distribution.	VIIIB2
receipting for	VIIIB2
registering of	VIIIB2a (2), IXC2, XB5
removal of, from Dept.	IXC2
storage of	IXB2, 5, XB, C
telegram	VIIIB2a (3), XIIIIC2
transmission of.	VIIIB2
Security	
daily inspections.	XC
plan for moves	XB7
Security Classification (see classified material)	
Security Messenger Service.	VIIIB1b (1), (3), (4), d (1), (2)
Security Officers, functions	
Department Security Officer.	IVA4, B2, 4, 8, VIIC2, D3b, c, VIIIB1b (5), d (1), IXB, XIIIG
Organizational Unit Security Officer	XA
Security procedures, instruction in	VIG
Special marking	VB, C
Storage, of classified material	IC14, VIID4, IXB, XB, C, XIB1, XIIIIF4, 5
System of Security Checks	XC

- 7 -

Telegrams	
as classified material	IC11, XIA, XIIIIA, B
classification of.	XIIIB
definition	IC11
disposal of copies	XI
distribution	VIIIB1, XIIIIC
downgrading.	IVB6
drafting	XIIIA
indicating classification of	VB
paraphrased versions	IIB2, IVB6
paraphrasing	XIIID
transmission of true reading	XIIIC3

Telephone, use of for classified information.	VIIIA
Tissue Sheet Copies, handling and storage of.	XB8
Top Secret material, information as a classification	IIIA
certification for access to	VIIIb1e
Classification procedure.	IVA1
Control Officer	VIIIb1e, IXC
definition and examples	IIIA
destruction, disposal of.	XIB
distribution outside Department	VIIC, D, VIIIb1d
handling.	VIIC, VIIIb1, XB, C
marking	VC3, VIIIb1
protection of	IXA, XB
storage	IXB1, 5
testimony	VIF2
Transmitting, transmission, of classified material	VIII, XIIIIC, F3
between organizational units.	VIIIb1b, 2a, 3a, 4a
Security Messenger Service (see Security Messenger Service)	
confidential material	VIIIb3
outside Department.	VIIIb1d, 2c, 3c, 4c
restricted material	VIIIb4
secret material	VIIIb2
to Foreign Service Post	VIIIb1c, 2b, 3b, 4b
to other Government Agencies.	VIID, VIIIb1d, 2c, 3c, 4c,
Top Secret material	VIIIb1
via Diplomatic Courier.	VIIIb1c (4), 2a (4), b (4)
via regular Messenger Service	VIIIb2, 3a, 4a, c
via responsible personnel	VIIIb1a (1), b (1), (2), (4), 2a (1), (2), (4), 3a (1), 4a
within Foreign Service.	VIIIb1b, 2a, 3a, 4a

- U -

Unclassified material, information marking	IIA
telegrams	IIIE, XIIIIA5
Upgrading, definition of	IC13

- V -

"Verbatim Text", marking on telegram	VC5
Visitors, outside of working hours	XIIC

- W -

Waste baskets, prohibited for disposal of classified material.	XIA
Waste material, classified disposal of	XIB