

AR 380-5**52-54 SAFEGUARDING MILITARY INFORMATION**

b. A message will be marked top secret, secret, confidential, restricted, or unclassified in accordance with its contents, except as prescribed in paragraph 58b(2).

53. Drafting messages.—a. Routine reports and messages which must be given a wide distribution, or the contents of which have been or may eventually be furnished the press, or which contain extracts or quotations from a newspaper, magazine, or any other document available to the public, will if possible be prepared so as to permit their transmission in the clear or will be cryptographed in special systems which permit the handling of the plain texts of the messages as correspondence of similar classification, otherwise, such reports and messages will be paraphrased in accordance with *d* below.

b. Standardization of the content and form of such documents as field orders and operation instructions is necessary, but when fixed expressions are repeated in a message, cryptographic security is greatly endangered. Hence stereotyped phraseology and set form of expression, especially at the beginning or ending of a message which is to be cryptographed will not be used. A list of words considered universally to be stereotyped is furnished by the War Department. Except as specifically provided for in certain cryptographic systems or as specifically authorized by the War Department, the use of dummy letters or irrelevant text as "padding" for the purpose of concealing stereotypic phraseology is prohibited. Personnel concerned with the drafting of classified messages will guard against repeated use of the same words or phrases.

c. Words not important to the sense will be omitted. Conjunctions, prepositions, and punctuation marks will be reduced to a minimum. Unless it is known that a message will be sent in clear text over an approved circuit or in a cryptographic system capable of enciphering punctuation marks as such, all punctuation marks included in the body of the message will be spelled either in full or abbreviated form. In similar circumstances, numbers will be also spelled out.

d. Except when it is known that a classified message will be sent in clear text over an approved circuit or in a cryptographic system not requiring the protection afforded by paraphrasing, the originator of all classified messages will paraphrase such portions as are quoted from—

- (1) A message in clear text.
- (2) A message in the same or another cryptographic system.
- (3) A newspaper, magazine, or document.

54. Selection of cryptographic system.—a. Cryptographic systems are supplied for handling messages of all classifications. All classified messages, except those transmitted in accordance with the provisions of paragraphs 25b and 58b(2), will be transmitted in cryptographed form, unless specific exception is made by the War Department.

b. Selection of the cryptographic system to be employed for the cryptographing of a message will be based on the following considerations:

- (1) A system authorized for the particular type and classification of message will be used.

- (2) Where all addressees can be reached by the same system, the least widely held system available will be used, unless a definite operational advantage will be gained by using a more rapid system for one or more of the addressees. Where all addressees cannot be reached by the same system, the same principle will be applied to the extent permitted by the available systems. Cryptographing of the same or related subject matter in different systems will be

SAFEGUARDING MILITARY INFORMATION

AR 380-5
54-56

kept to a minimum. Headquarters or commands in frequent communication should normally use the same system for exchange of the same type of messages.

c. The determination of the need for paraphrased versions is a function of the cryptographic security officer who may require the assistance of the originator of the message in the preparation of the necessary paraphrases. Where practicable, the cryptographic security officer will furnish copies of the paraphrased versions to the originator, except as noted in paragraph 48b.

55. Paraphrasing messages.—a. In paraphrasing, it is not sufficient to paraphrase only the beginning or ending of the message. The entire message will be subjected to the process.

b. When paraphrasing must be employed, all of the following processes will be applied to the message:

- (1) Changing the sequence of the paragraphs.
- (2) Changing the sequence of the sentences in each paragraph.
- (3) Shifting the positions of the subject, predicate, and modifiers in each sentence.
- (4) Changing from active to passive voice or vice versa.
- (5) Substituting synonyms or equivalent expressions.
- (6) Changing the length of the paraphrased version of the message in order that the final cipher text will not resemble the original cipher text with respect to length.

c. A paraphrase of a message normally will be accorded the same classification as the original message.

56. Method of handling outgoing secret messages.—a. The procedure hereinafter described will be followed at all headquarters, except the War Department in which the procedure will be as determined by the Chief of Staff.

b. Except as noted in c below or as authorized in accordance with the instructions pertaining to certain cryptographic systems issued by the War Department, the originator will prepare and number all copies of secret messages, send the original to the message center, and may retain, when security is not imperiled thereby, one copy for temporary file. Other carbon copies, all numbered and bearing the following notation, may be sent to local officers directly concerned:

The making of an exact copy of this message is forbidden. Only such extracts as are absolutely necessary will be made and marked SECRET. This copy will be safeguarded with the greatest care and will be returned to the originator without delay.

All such copies will be carefully accounted for by the originator and will be destroyed when returned. The copy in the temporary file will also be destroyed upon determination that the message has been correctly dispatched.

c. Messages pertaining to tactical operations, simulated or actual, may be prepared in triplicate. One carbon may be retained by the originator and the original and one carbon delivered to the message center.

d. The original plain-text copy sent to the message center by the originator will be cryptographed at the cryptographic section of the message center. The number of copies of the cryptographed message will be kept at a minimum commensurate with the necessity for furnishing copies to the various transmission agencies. All work sheets used in cryptographing the message will be destroyed by burning. The placing on the original plain-text copy of any marks or notations to indicate the steps following in cryptographing the message, such as underlining key words, indicating groupings corresponding to lengths of columns

AR 380-5**56-58 SAFEGUARDING MILITARY INFORMATION**

of keys, etc. is forbidden. All copies of cryptographed messages retained by transmitting agencies will be safeguarded so as not to fall into unauthorized hands.

e. The original copy of the literal plain text will be marked SENT (date) and returned to the originator who will place it in his secret file for outgoing messages and destroy the retained copy by burning.

f. The transmitting agency will send the cryptographed message, retaining at least one copy in its file of outgoing messages for final disposition in accordance with local regulations.

g. When certain cryptographic systems are used in which no copy of the cipher text is available, a copy of the plain text may be retained by the message center for file.

h. The method of handling top secret messages will conform to the procedure outlined above as modified by the provisions of paragraph 27a(2) and (3).

57. Method of handling incoming secret messages.—a. The procedure hereinafter described will be followed at all headquarters, except the War Department in which the procedure will be as determined by the Chief of Staff.

b. The original copy of an incoming cryptographed message as made by the receiving operator will go to the cryptographic section of the message center. A duplicate copy may be made by the receiving operator for the files of the receiving station or message center, where it will be disposed of in accordance with local regulations.

c. A cryptographer will decryptograph the message, making only one copy of the decryptographed literal plain text, which will be marked SECRET and delivered to the addressee. The cryptographed version will be retained in the files of the message center, where it will be disposed of in accordance with local regulations. All work sheets used in decryptographing will be destroyed by burning. The cryptographic section will not retain any copy of the plain text for its files, except as provided in paragraph 56g. The placing on the message blank of any marks or notations to indicate the steps followed in decryptographing the message, such as underlining key words, indicating groupings corresponding to lengths of columns of key, etc., is forbidden.

d. Except where authorized in accordance with instructions pertaining to certain cryptographic systems issued by the War Department, the addressee may make and circulate only a limited number of literal copies for the information of other officers directly concerned. These carbon copies will all be numbered and bear the following notation:

The making of an exact copy of this message is forbidden. Only such extracts as are absolutely necessary will be made and marked SECRET. This copy will be safeguarded with the greatest care and will be returned to _____ without delay.

All such information copies will be carefully accounted for by the addressee and will be destroyed when returned.

e. The method of handling top secret messages will conform to the procedure outlined above as modified by the provisions of paragraph 27a(3).

58. Method of handling outgoing and incoming confidential messages.—a.—*Procedure.*—The procedure to be followed in the handling of messages in confidential codes or ciphers will be substantially the same as that prescribed for those transmitted in secret code or cipher, except within the War Department, in which the procedure will be as determined by the Chief of Staff. They will, however, be marked and safeguarded in accordance with provisions of these regulations governing confidential documents.

AR 380-5

SAFEGUARDING MILITARY INFORMATION 58-60

b. In tactical operations, simulated or actual.

- (1) All messages not classified secret will be regarded as confidential but need not be so marked. All wire and radio messages except those noted in (2) below will be transmitted in cryptographic form.
- (2) When the information to be transmitted, if intercepted by the enemy, cannot be acted upon in time to influence the situation in question and time cannot be spared for cryptographing, the commanding officer or his authorized representative may order the transmission of a message in plain language by a radio station serving his headquarters or command. Such written messages will be marked **SEND IN CLEAR** over the signature of the commander or his authorized representative.

59. Method of handling restricted messages.—The procedure to be followed in the handling of messages in restricted codes and ciphers will be substantially the same as that prescribed for those in confidential code or cipher.

60. Transmission of literal plain text and paraphrased versions of classified messages.—*a.* The sending by any means whatsoever of the literal plain text of a message which has been or will be transmitted in cryptographed form is strictly prohibited except as stated below:

- (1) Authorized specifically by the War Department.
- (2) Authorized local distribution within a headquarters by messenger.
- (3) In exceptional cases, when necessary in the performance of his duties, an authorized person may carry the literal plain text of a classified message provided the security requirements pertaining to the transmission of classified material are observed.
- (4) Where authorized in accordance with instructions pertaining to certain cryptographic systems issued by the War Department.

b. In cases of emergency or necessity paraphrased versions of the plain text of a cryptographed message will be sent—

- (1) In accordance with the provisions of paragraphs 51*f* and 55*c*.
- (2) In accordance with the provisions of paragraph 26 as applied to secret cryptographic material.
- (3) When it is necessary to send between headquarters by mail or courier a paraphrased copy of a message which has been or will be cryptographed, copy will be marked or stamped "This is a paraphrase."

SECTION V
MATÉRIEL

	Paragraph
Authority to classify.....	61
Notification of classification or reclassification.....	62
Responsibility for safeguarding technical information.....	63
Classification of information from commercial firms.....	64
Dissemination of classified technical information.....	65
Destruction of classified matériel.....	66
Invitations for bids and contracts.....	67
Consultations with responsible manufacturers.....	68
Responsibility of Army representatives or inspectors.....	69
Responsibility of Government contractors.....	70
Tests of classified matériel.....	71
Public display of classified matériel.....	72
Release of information or sale of matériel.....	73
Protection of shipments via commercial carriers within United States or its possessions.....	74

AR 380-5**61-66 SAFEGUARDING MILITARY INFORMATION**

61. Authority to classify.—Whenever the chief of a technical service responsible for a research project or for the design, development, test, or production or procurement of an article of matériel or a component thereof shall determine that the maintenance of any degree of secrecy regarding them is sufficiently important to the national defense, he will classify it as top secret, secret, confidential or restricted.

62. Notification of classification or reclassification.—Whenever the chief of a technical service in charge of a research project, design, development, test, or production of a unit of matériel or component thereof shall determine that matériel of interest to other commands should remain classified after issue or that a change or cancellation of classification is desired, he will notify The Adjutant General, who in turn will inform all concerned.

63. Responsibility for safeguarding technical information.—*a.* Chiefs of technical services engaged in the preparation of plans, research, and development work, or new design, test, production, procurement, storage, or use of classified matériel are responsible for the promulgation of such additional instruments as may be required for the safeguarding of information in the offices, establishments, laboratories, shops, or Army posts under their jurisdiction.

b. All top secret, secret, confidential, or restricted models, exhibits, dies, machines, and other similar items which are to be loaned, leased, or given to a commercial organization will be properly marked to indicate classification when practicable. If such marking is impracticable, the commercial organization will be specifically notified in writing of the classification of such items and of the pertinent provisions of the Espionage Act.

64. Classification of information from commercial firms.—Information obtained from civilian manufacturers concerning proprietary processes will be classified as confidential unless otherwise authorized by the firm concerned.

65. Dissemination of classified technical information.—Classified information concerning technical projects or developments may be imparted only to those individuals whose official duties require such knowledge or possession, and to accredited representatives of foreign nations in accordance with the provisions of paragraph 20*b*.

66. Destruction of classified matériel.—*a. Authority to direct.*—Whenever the chief of a technical service responsible for a research project or for the design, development, test, or production or procurement of an article of matériel or a component thereof shall determine that their destruction is necessary to safeguard information thereof, he will issue the necessary directive.

b. Procedure in destruction of classified matériel.—When destruction of classified matériel has been directed—

- (1) The custodian thereof will remove all components of a classified nature and destroy them by burning or by mutilation in the presence of a disinterested officer. The balance of the matériel will then be processed in accordance with existing regulations for the disposition of unserviceable property, or for salvage.
- (2) If the above is not practicable, the custodian will destroy the entire article of matériel by burning or by mutilation in the presence of a disinterested officer.
- (3) In either case, the certificate of destruction will be signed by both the custodian and the witnessing officer before submission to the officer directing the destruction. If the headquarters has only one com-

AR 380-5
SAFEGUARDING MILITARY INFORMATION 66-67

missioned officer, the report will so state. Exception hereto may be authorized only by the War Department.

67. Invitations for bids and contracts.—*a.* Prior to furnishing a prospective bidder, subbidder, contractor, or subcontractor with drawings, specifications, or other pertinent information concerning any project or projects of a top secret, secret, confidential, or restricted nature and annually thereafter so long as such documents, etc., are in his custody, clearance will be obtained in accordance with separate letter instructions and a general secrecy agreement reading substantially as follows will be signed by the individual or by a responsible officer on behalf of the firm or corporation concerned:

In consideration of the receipt of drawings, specifications, and accompanying inclosures, models, or matériel, and information disclosed orally, concerning projects of a top secret, secret, confidential, or restricted nature, delivered to the undersigned prior to or coincident with the date of this agreement and listed on Exhibit A which is attached hereto and made a part hereof, or to be issued to the undersigned subsequent to the date of this agreement, the following terms are agreed to by or on behalf of the undersigned individual, firm, or corporation, and any and all representatives, agents, employees, or subbidders or subcontractors thereof:

1. The undersigned will neither supply nor disclose any information regarding the drawings, specifications, and accompanying inclosures or models or matériel, or information disclosed orally, referred to herein to any unauthorized person, or incorporate in other projects special features of design or construction peculiar to such drawings, specifications, and accompanying inclosures, or models or matériel, or information disclosed orally.

2. (a) The undersigned will *not permit any alien* employed or to be employed by the undersigned or by any subbidder or subcontractor to have access to the drawings, specifications, and accompanying inclosures, or models or matériel referred to herein, or to engineering principles, compositions, subassemblies, or assemblies which are vital to the functioning or use of the article or to the work under any contract for the production thereof, or to work in connection with the contract trials, without the written consent *beforehand* of the Secretary of War.

(b) If the project or projects bear a top secret or secret classification, the undersigned will *not permit any individual* to have access to the top secret or secret drawings, specifications, and accompanying inclosures, or models or matériel referred to herein, or to the top secret or secret engineering principles, compositions, assemblies, or subassemblies, or to work under any contract for the production of such top secret or secret items, or to work in connection with the contract trials, without the written consent *beforehand* of the Secretary of War.

3. The undersigned will not make or permit to be made reproductions of the drawings, specifications, and accompanying inclosures, or of the models or matériel, except as specifically authorized by the contracting officer or his duly authorized representative. If reproduction of any drawings, specifications, and accompanying papers, or of models or matériel, is authorized, the undersigned will promptly submit the product obtained to the contracting officer or his duly authorized representative for censorship or such other action as he may deem necessary.

4. If a bid is not submitted on a project of a top secret, secret, confidential, or restricted nature as to which classified drawings, specifications, and accompanying inclosures, and models or matériel have been issued to the undersigned, or if a bid is made and not accepted, or in case award is made, upon the completion of the contract, the undersigned will promptly return by hand, by registered mail, or by insured express, such drawings, specifications, and accompanying papers, or models or matériel, together with all copies thereof, to the office from which the original copies were received. Registered mail or insured express will not be used in returning top secret matter.

5. (a) The undersigned agrees to bring or cause to be brought to the attention of all persons engaged in the preparation of the bid, whether submitted or not, including subbidders and their employees, the following provisions of law:

AR 380-5

67

SAFEGUARDING MILITARY INFORMATION

Espionage Act: Subparagraphs (d) and (e), sec. 1, act 15 June 1917 (40 Stat. 217); sec. 1, act 28 March 1940 (54 Stat. 79; 50 U. S. C. 31; M. L., 1939, Supp. I, sec. 2181).

Sec. 1, act 12 January 1938 (52 Stat. 3; 50 U. S. C. 45; M. L., 1939, sec. 2187a), and E. O. 8381, 22 March 1940; 5 F. R. 1147; 50 U. S. C. 45; M. L., 1939, Supp. III, sec. 2187a.

Second War Powers Act, 1942, sec. 1402, 1403, act 27 March 1942 (Public Law 507-77th Cong.), as extended by act 20 December 1944 (58 Stat. 827; 50 U. S. C. Supp. IV, sec. 645).

(b) If the successful bidder on any project, the undersigned agrees also to bring or cause to be brought to the attention of all persons engaged in the performance of the contract, including persons employed on subcontracts, the provisions of the law enumerated in (a) above.

6. The undersigned further agrees that no information in connection with any confidential or restricted project will be given to any person not in the contractor's or subcontractor's employ except upon the written consent beforehand of the contracting officer or his duly authorized representative.

b. The execution of the general secrecy agreement required in a above with any individual, firm, or corporation whether it be the prime contractor or subcontractor, prior to the delivery of any classified military information, and the annual secrecy agreements executed thereafter, will constitute authority for delivery to such individual, firm, or corporation from time to time of other or additional classified information pertaining to any top secret, secret, confidential, or restricted project, without the necessity of executing a specific secrecy agreement in each case. A receipt substantially as follows will be obtained when the additional classified data are submitted to those who have entered into such agreement:

Receipt is acknowledged of _____ and it is recognized that these data are classified and come within the purview of the secrecy agreement signed by _____ on _____.

c. If the project(s) or contract(s) bear a top secret or secret classification, two copies of the executed secrecy agreement or agreements and two copies of each annual secrecy agreement executed thereafter will be transmitted promptly by the procuring agency to the commanding general of the army within the area in which the work will be, or may be, performed. The commanding general of the army concerned will retain one copy and forward one copy to the Provost Marshal General.

d. It is the responsibility of each representative of the War Department who invites bids in connection with a project or projects of a top secret or secret classification, to transmit promptly the following information in duplicate to the commanding general of the army within the area in which the work will be, or may be, performed:

- (1) The name and addresses of each prospective bidder or subbidder.
- (2) The address; full first and last names and middle initial; date and place of birth, of each officer and director and of all persons who will have access to the top secret and secret matériel.
- (3) The location of the facility at which the work involved will be, or may be, performed.
- (4) The date of invitation for bids.

e. It is the responsibility of each representative of the War Department who enters into a contract classified as top secret or secret, to transmit promptly the following additional information in duplicate to the commanding general of the army within the area in which the work will be, or may be, performed:

AR 380-5

SAFEGUARDING MILITARY INFORMATION 67-70

- (1) The name and address of each contractor or subcontractor.
- (2) The address; full first and last names and middle initial; date and place of birth, of each employee or other person who will have access to the top secret or secret matériel not included in *d* (2) above.
- (3) The location of the facility at which the work involved will be, or may be, performed.
- (4) The date of award of contract or subcontract, and probable date of commencement of work thereunder.

f. The commanding general of the army concerned will retain one copy and forward one copy of the reports received in accordance with *d* and *e* above, to the Provost Marshal General.

68. Consultation with responsible manufacturers.—The commanding officers of arsenals and depots and other officers engaged in work on Government contracts are authorized to consult with all interested manufacturers or their representatives, inventors, and other persons concerning technical matters in which they have a legitimate interest. They will, however, inform all such persons of the classification of the projects, works, and developments.

69. Responsibility of Army representatives or inspectors.—*a.* The Army representatives or inspectors of the technical service are the local representatives of the War Department and will take the necessary measures to insure the safeguarding of classified information or projects in the hands of the contractors or subcontractors or in process of manufacture in their plants.

b. Army representatives or inspectors will advise contractors or subcontractors as to their responsibilities and the practical measures to be taken to safeguard top secret, secret, confidential, or restricted matters, and will act favorably, if practicable, on any suggestion or request of the company tending to preserve secrecy. If at any time conditions at any plant, or any action of a company or its employees, jeopardize the security of classified matter pertaining to the War Department or violate the provisions of the Espionage Act, the Army representative or inspector will request the contractor or subcontractor to take prompt remedial action. If adequate precautionary measures are not taken immediately, he will report promptly to the chief of the technical service concerned and, if the situation requires, to the commanding general of the army in which the item is in process of manufacture.

c. When Army and Navy inspectors are on duty at the same plant, the Army inspector will coordinate all security measures with the Navy inspector in order to avoid conflicting demands upon contractors.

70. Responsibility of Government contractors.—*a.* A private individual, firm, or corporation which enters into a contract to engage in technical work for the War Department becomes responsible in matters within his or its control for the safeguarding of all top secret, secret, confidential, or restricted matters that may be disclosed or that may be developed in connection therewith. A clause to this effect will be included in such a contract, but its omission will not release the contractor from his responsibility under the Espionage Act and other pertinent laws.

b. Contractors are responsible that all classified projects allotted to subcontractors or agents are fully protected by a similar agreement.

c. Whenever for any reason a contract agreement or subcontract has been made which does not include a security clause but later is found to involve top secret, secret, confidential, or restricted matter, the technical service concerned will take the necessary steps to insure that the project or work is properly

AR 380-5**70-74 SAFEGUARDING MILITARY INFORMATION**

classified and that the contractor, agent, or subcontractor is informed of the classification and of his responsibility in the matter.

71. Tests of classified matériel.—Tests of classified matériel will be adequately safeguarded by all responsible officers.

72. Public display of classified matériel.—*a.* Commanding officers are responsible that all classified parts, components, or features of matériel are properly safeguarded during maneuvers, drills, parades, ceremonies, assemblages, demonstrations, or exhibitions, or exhibitions, open to the general public.

b. (1) Photographs of equipment while in process of development or those revealing processes of manufacture are prohibited unless authorized by the chief of technical service concerned. After an article of equipment has been issued to combat units, release of photographs is permissible unless specifically prohibited by the instructions issued therewith.

(2) Requests for permission to take photographs of classified matériel, projects, or processes of manufacture will be referred to the War Department through the proper chief of technical service. If authority is granted, it will be with the understanding that the resulting photographs will be submitted to the War Department for review prior to release.

73. Release of information or sale of matériel.—*a. General.*—Domestic sale, divulging information in connection with negotiations for foreign sale, and foreign manufacture of items of Army and Navy matériel and equipment are not permitted unless the War and Navy Department are agreed that military secrecy is not compromised thereby.

b. International traffic in arms.

(1) The State Department administers international traffic in arms and military matériel coming within the scope of the Regulations Governing the International Traffic in Arms, Ammunitions, and Implements of War and Other Munitions of War.

(2) The State Department will not release for foreign sale any item within the scope of these regulations until the War and Navy Departments have stated that there is no objection to the release on grounds of secrecy affecting the national defense.

74. Protection of shipments via commercial carriers within United States or its possessions.—*a. Selection of shipping method.*—Disclosure of information pertaining to classified matériel will be prevented during transportation by one of the following methods of shipment, to be determined by a commissioned officer of the service, force, or organization authorizing its movement qualified to make such classification, by a higher authority so qualified, or by a military attaché.

b. Protection documents.—If size and quantity permit, classified matériel may be handled in the same manner as provided for similarly classified documents in paragraphs 26 to 29 inclusive. In cases where matériel is of such size or quantity as to create suspicion of its character and entail additional risk when transported in the same manner as documents, another method will be used.

c. Railway express service protected by carrier's guards.—Top secret, secret, or confidential shipments may be shipped via Railway Express Agency, Incorporated, after advance arrangements have been made for carrier to guard matériel from the time it leaves the hands of consignor until delivered to consignee. Notwithstanding the general prohibition of insurance on Government shipments any classified shipments may be shipped at their actual value and notation of such

SAFEGUARDING MILITARY INFORMATION

AR 380-5

74

value made on the bills of lading. (See AR 55-105, AR 55-155, and TM 55-550.) The officer determining the method of shipment will certify to the officer issuing the bill of lading the valuation to be used.

d. Ordinary railway express service protected by military guards.—This method of shipment may be chosen for top secret, secret, or confidential matériel as provided in *a* above. In such case the principles of regulations governing guarding of freight shipments (see par. 8, AR 55-155) will be followed so far as appropriate for express service, with the definite exception that guards with express shipments will be furnished with transportation requests. The number of guards detailed to protect the shipment will be a minimum consistent with security requirements.

e. Air express via commercial air lines protected by military guards.—The provisions of *d* above will govern generally.

f. Rail freight service protected by military guards.—See paragraph 8, AR 55-155.

g. Ordinary motor truck freight protected by military guards.—The principles of paragraph 8, AR 55-155, will govern. Only one guard will be used for short runs unless more are necessary.

h. Water freight service protected by military guards.—The principles of paragraph 8, AR 55-155, will govern. When vessels are used which have arrangements for carrying passengers, transportation requests will be issued. When vessels are used which do not have arrangements for carrying public passengers, carriage free or at a reasonable charge, appropriate arrangements for meals will be negotiated.

i. Straight or mixed troop trains.—Classified matériel accompanying troops will be adequately guarded by organization personnel.

j. Guards.—Guards sufficiently armed will be provided in accordance with paragraph 8, AR 55-155. Neither carrier's nor military guards will be used for the sole purpose of preventing disclosure of information of restricted matériel. Guarded service may be used on any shipment when necessary to prevent physical sabotage. When possible, where concealment of the arm is not necessary, submachine guns, automatic rifles, or rifles should be provided in preference to pistols.

k. Shipment, confidential matériel without guard.—Shipments of confidential matériel, except cryptographic equipment and components thereof may, at the discretion of the chief of the technical service involved, be shipped by one of the following methods, without guard:

- (1) Protected express.
- (2) Sealed freight or express cars.
- (3) Sealed truck under own motive power.
- (4) Flat car, provided trucks or crates containing said equipment are suitably locked and/or sealed and locked and/or sealed to the car. In addition, the equipment will be protected from external view and injury from normal hazards in shipping.

l. Shipment, restricted matériel without guard.—Shipments of restricted matériel, except cryptographic equipment and components thereof, may be shipped by one of the following methods, without guard:

- (1) Protected express.
- (2) Sealed freight or express cars.
- (3) Sealed truck under own motive power.
- (4) Flat car, provided trucks or crates containing said equipment are suitably locked and/or sealed and locked and/or sealed to the

AR 380-5

74-76

SAFEGUARDING MILITARY INFORMATION

car. In addition, the equipment will be protected from external view and injury from normal hazards in shipping.

m. Shipment, cryptographic matériel.—For specific means of shipments of cryptographic matériel reference should be made to letter instruction on this subject issued by the War Department.

n. Shipment, classified files.—Shipments of classified files to records depots and War Department records depositories will be made as follows:

- (1) When the quantity of top secret, secret, or confidential documents remaining after down grading is small, the documents will be transmitted under separate cover as provided elsewhere in these regulations for the transmission of individual documents. A charge-out will be placed in the folder which contained the document and the document will be properly identified as to the file and folder from which extracted prior to transmission.
- (2) When the quantity of top secret, secret, and confidential documents which cannot be down graded makes the procedure above impracticable, the files in which such documents are maintained will be packed in the standard records boxes prescribed by TM 12-259, securely fastened by flat steel straps. The outside of the box will contain no indication of the classified character of the files. The boxes will be shipped under security regulations applicable to bulk shipments of classified matériel except that top secret and cryptographic documents and messages in all cases will be accompanied by an officer courier in addition to armed guards.
- (3) Shipment of restricted files. Such files will be shipped in standard records boxes in the same manner as prescribed for unclassified files.

SECTION VI**VISITORS**

Classification	Paragraph
Authority for admission.....	75
Responsibility of commanding officer, Army representative, or inspector.....	76
Responsibility of Government contractors.....	77
	78

75. Classification.—*a. Foreign nationals.*—For the purpose of these regulations, the term "foreign nationals" includes all persons not citizens of the United States, and citizens of the United States while a representative, official, or employee of a foreign government, firm, corporation, or individual.

b. United States citizens.—All citizens of the United States not included in *a* above.

76. Authority for admission.—*a. General.*—Correspondence and communications relating to visits will be routed direct between the various offices concerned.

b. Foreign nationals. (See par. 75a.)

- (1) Subject to the approval of the facility concerned, foreign nationals may be authorized by local authority to visit commercial facilities provided no classified work or project is shown or discussed.
- (2) Foreign nationals may be admitted to military installations for social purposes, for activities open to the general public, and in connection with emergency landings, by authority of the commanding officer provided no classified features are shown or discussed.

AR 380-5

SAFEGUARDING MILITARY INFORMATION

76

(3) Foreign nationals may be admitted to Government facilities; military installations except as provided in (2) above; and commercial facilities where classified work, projects or features will be shown or discussed, only on written authority of the Director of Intelligence, War Department General Staff.

(4) Application for visits which require War Department authorization will be made through the appropriate diplomatic representatives, except in the case of foreign nationals employed by citizens of the United States or by firms or corporations owned or controlled by citizens of the United States for whom applications will be submitted by their employers, approved by the commanding officer or management of the facility to be visited, and forwarded with the recommendation of the chief of the technical service or appropriate commanding general of the army concerned to the Director of Intelligence, War Department General Staff, who will secure the recommendation of the Navy Department. Applications submitted through either of the channels described above will include the following information:

- (a) Name in full.
- (b) Official title or position.
- (c) Name of plant or plants, posts, camps, or airfields to which admission is desired.
- (d) Date of visit or dates between which visits are desired.
- (e) Purpose of visit.

For foreign nationals employed by citizens of the United States or by firms or corporations owned or controlled by citizens of the United States the following additional information will be required:

- (f) Nationality.
- (g) Length of service with present employer.

(5) Prior to authorizing a visit to a War Department installation or to a commercial facility where classified work, projects, or features will be shown or discussed, the Director of Intelligence, War Department General Staff, will secure the recommendations of the Navy Department and the chief of the technical service concerned. Members of the armed forces of Canada and Mexico may, however, be admitted to Army posts, camps, and airfields near the borders of those countries for occasional visits on the authority of the commanding general of the army, defense command, or air force command having jurisdiction over such posts, camps, or airfields, without reference to higher authority.

c. United States citizens.—Subject to the approval of the commanding officer or the contractor, United States citizens, except those representing a foreign government, firm, or corporation, may be admitted to War Department or commercial manufacturing establishments engaged on classified work or projects under the following conditions:

- (1) Casual visitors may be admitted provided no classified work or project is shown or discussed.
- (2) Representatives of other United States Government agencies, manufacturers, or their representatives, engineers, and inventors cooperating in War Department work and having a legitimate interest

AR 380-5

77-78

SAFEGUARDING MILITARY INFORMATION

therein may be shown such works or projects as are considered necessary and desirable by the responsible chief of technical service. Authority for admission will be in writing.

- (3) Accredited reporters, photographers, and other representatives of publicity agencies may be admitted to War Department installations or manufacturing establishments engaged on work for the War Department, *provided*, classified matter, projects, or processes of manufacture are not shown or discussed with them.

77. Responsibility of commanding officer, Army representative, or inspector.—*a.* The commanding officer of a military establishment or the Army representative or inspector at a commercial establishment is the local representative of the War Department in all matters regarding the admission of visitors. If, in his opinion, the situation at the time makes the admission of a visitor inadvisable, he is empowered to postpone the visit and request instructions from the office which authorized it.

b. The commanding officer or Army representative will make a report to the Director of Intelligence, War Department General Staff, through the appropriate chief of technical service or commanding general of the army concerned, giving the following information concerning foreigners who visit establishments engaged in classified projects:

- (1) Name, official position, and nationality.
- (2) Authority for the visit.
- (3) Matters in which the visitors showed the greatest interest.
- (4) General nature of questions asked.
- (5) Expressed object of the visit.
- (6) Inspector's estimate of the real object of the visit.
- (7) General estimate of ability, intelligence, and technical knowledge of the visitor and his proficiency in the English language.
- (8) A brief list of what was shown and explained.

78. Responsibility of Government contractors.—*a.* Contractors or subcontractors engaged in work for the War Department must place such restrictions on the movements of persons employed or entering their plants or offices as will give adequate security to top secret, secret, confidential, or restricted matters in their possession. In view of the wide differences in organization, arrangement, and physical make-up of individual plants, no specific rules are practicable. Therefore, local conditions at the plant and the classification of the project will determine the security measures to be adopted.

b. The following general procedure in regard to visitors at establishments or plants engaged in classified projects for the War Department is prescribed:

- (1) Visitors will be accompanied during their stay at the plant by the inspector or Army representative, a member of his office, or some responsible person who is specifically informed as to the necessary limitations or restrictions, the scope of the visit, and the information which may be furnished.
- (2) Unless specifically authorized by the authorities mentioned in paragraph 76, visitors will not be allowed in any shop, laboratory, drafting room, or section of a plant where top secret, secret, confidential, or restricted matériel is located or where classified work is in progress, nor will they be permitted to take photographs.

AR 380-5

SAFEGUARDING MILITARY INFORMATION

78-80

- c. (1) War Department contractors will submit to the commanding general of the army or chief of technical service, whichever is appropriate, immediately upon completion of the visit, a report of all visitors, except United States citizens, who have gained information concerning the classified work or projects. The reports will include the following information:
 - (a) Name, official position, and nationality.
 - (b) Authority for visit.
 - (c) Matters in which the visitors showed the greatest interest.
 - (d) General nature of questions asked.
 - (e) Expressed object of the visit.
 - (f) Estimate of the real object of the visit.
 - (g) General estimate of ability, intelligence, and technical knowledge of the visitor and his proficiency in the English language.
 - (h) A brief list of what was shown and explained.
- (2) The commanding general of the army or chief of technical service, whichever is appropriate, will submit the reports to the Director of Intelligence, War Department General Staff, through the appropriate chief of technical service.

SECTION VII

AIR SPACE RESERVATIONS, RESTRICTED AREAS, AND RESERVED AREAS

Air space reservations.....	Paragraph
Restricted areas.....	79
Reserved areas; establishment.....	80
	81

79. Air space reservations.—*a. Establishment.*—Air space reservations over military installations or reservations over which the flight of aircraft is prohibited or restricted for the purpose of national defense or for other governmental purposes are established by executive order of the President of the United States, or by a State, Commonwealth, or Territory.

b. Responsibility of commanding officers.—The commanding officer of a military reservation, post, camp, station, or installation over which an air space reservation has been established is responsible for the surveillance of the designated air space and for prompt report to The Adjutant General, through military channels, of any illegal flight therein.

80. Restricted areas.—*a. Designation.*—The commanding officer of a military reservation, post, camp, station, or installation is responsible for the designation and proper safeguarding of restricted areas in his military reservation, post, camp, station, or installation. If local conditions dictate, he will mark all ordinary entrances or approaches to such areas with a sign reading as follows:

WARNING

RESTRICTED AREA

It is unlawful to enter within this _____ without written permission of _____ (Area, building, etc.)
 _____ (Authority)

AR 380-5
80-82

SAFEGUARDING MILITARY INFORMATION

b. Procedure in case of violation.

- (1) The commanding officer of a military reservation, post, camp, station, or installation will cause any person not subject to military law who enters a restricted area or building to be detained, warned of his rights, and interrogated by proper authority. If it is a first offense and there is no evidence of deliberate intent, the offender may be warned against repetition and released upon the surrender of any unlawful photograph, sketch, picture, drawing, map, or graphic representation in his possession. Otherwise the offender will be delivered without unnecessary delay to the nearest United States marshal with a written statement of the facts, the names and addresses of the witnesses, and such pertinent exhibits as may be available.
- (2) When an investigation reveals that a person not subject to military law has entered such a restricted area or building, custody of the individual not having been effected, the commanding officer will promptly forward in writing to the nearest United States district attorney a report of all the facts, including the names and addresses of the witnesses.
- (3) A report will be made through military channels to the commanding general of the army concerned of each case brought to the attention of civil authority and will include a brief of all the facts and copies of all pertinent communications.

81. **Reserved areas; establishment.**—Areas reserved for military or national defense purposes, admittance to which is either restricted or prohibited, are set apart by executive order of the President of the United States or by order of the Secretary of the Interior.

SECTION VIII

TROOP MOVEMENTS, INDIVIDUAL TRAVEL, AND MOVEMENT OF SUPPLIES

	Paragraph
General.....	82
Classification requirements.....	83
Dissemination of information.....	84
Rail and motor movements.....	85
In staging areas.....	86
Embarkation.....	87
Movement of vessels in harbors.....	88
At sea.....	89
Returns to continental United States.....	90
Movements by air.....	91
Theater of operations in continental United States.....	92
Higher classification.....	93
Reason for classification.....	94
Periods of peace or following termination of hostilities.....	95

82. **General.**—*a. Application.*—The provisions of *b* below and paragraphs 83 to 94 inclusive, will apply during periods of hostilities. The provisions of paragraph 95 will apply during periods of peace or following the termination of hostilities and before peace is formally declared.

b. Responsibility of commanding officers.—Commanding officers of units, replacements, or individuals affected by the provisions of this section are responsible that such personnel are instructed in these provisions, advised of their appli-

SAFEGUARDING MILITARY INFORMATION

AR 380-5
82-83

cability, and warned of the danger involved in the disclosure to unauthorized persons of classified information concerning troop movements or movement of supplies. Necessary instructions will be given both at home station and staging area prior to movement to a theater of operations.

83. Classification requirements.—a. Movement of personnel or supplies.—Information of movements of personnel or supplies will be classified, when appropriate, as secret, confidential, or restricted by, or by authority of, any officer authorized to make or authorize secret classifications under paragraph 10a. In order to insure proper and uniform classification, it is essential that documents concerning movements be classified, when appropriate, in accordance with the principles contained in this section.

b. Troop movements or travel of replacements to theater of operations.—The following elements of information concerning troop movements or travel of replacements or individuals to a theater of operations will normally be classified as indicated, except as stated in paragraph 91:

- (1) *Secret.*—Documents which contain any one of the following elements, either directly or by implication, require a classification of secret:
 - (a) Oversea or intertheater destination in the clear, when such destination is an active theater of operations or a specific location within an active or inactive theater of operations.
 - (b) A specific port of destination within continental United States for return to continental United States in travel by water.
 - (c) Date and time of departure from a port of embarkation, a port of debarkation en route, a port of aerial embarkation, or a port of aerial debarkation en route.
 - (d) Route, name, or destination of ship or convoy.
 - (e) Estimated time of arrival at an overseas or intertheater destination, or at ports or airports of debarkation en route.
 - (f) The meaning of an assigned shipment number so far as it represents a specific overseas or intertheater destination.
 - (g) The overseas or intertheater destination represented by a temporary APO number.
 - (h) Events en route involving enemy action.
- (2) *Confidential.*—Documents which contain any of the following elements will be classified confidential:
 - (a) Inactive theater of operations as a destination, in the clear, provided the exact destination within the theater is not shown.
 - (b) Information or description of unit movements of nonoperational significance within areas in or adjacent to active theaters of operations.
 - (c) A list or tabulation of two or more units combined with and included under a single shipment number or other comparable code designation. The combination of a single unit with its overseas shipment number and letter, or other comparable code designation, however, is restricted information.
- (3) *Restricted.*—The following types of information, or documents containing this information, except as indicated in (1) and (2) above, will normally be classified restricted:
 - (a) Orders, communications, reports, and other documents con-

AR 380-5

83

SAFEGUARDING MILITARY INFORMATION

cerning troop movements, oversea or domestic travel of replacements, or oversea travel of individuals. However, reports and communications concerning movements need not be classified if the classified elements of information and unit designations are not included therein and reference to the movement is made by shipment number and letter (or other comparable code designation), by temporary APO number, or by main number.

(b) Troop movements between inactive theaters of operations, between the United States and inactive theaters of operations, within inactive theaters of operations, and domestic troop movements within continental United States, provided such movements are not associated with further movement to an active theater of operations.

(c) Continental United States as a destination in the clear, provided the specific port of debarkation in travel by water is not shown.

c. Domestic travel within continental United States.—Domestic travel within continental United States of individuals which is not associated with further movement to a theater of operations or with classified activities will not normally require classification.

d. Movement of supplies.

(1) Movements of supplies and impedimenta which are to accompany units, or are destined for, or otherwise associated with specific units or specific troop movements will be governed by the classification requirements set forth in *b* above.

(2) Movements of supplies which are not associated with specific units or troop movements:

(a) Movements will normally carry a coded destination symbol such as a shipping designator or shipment number. Documents covering such shipments which by inference or by literal reference compromise the meaning of the coded destination symbol will require a classification at least as high as that of the meaning of such coded symbol.

(b) Movements may be addressed in the clear to oversea destination when authorized by the Secretary of War. This method of addressing will not normally be used when the presence of military installations such as oversea ports, combat airfields, harbor defenses, or similar establishments will be exposed thereby.

(c) When a coded designation of specific shipments, projects, or locations, such as a consignee combination, is used in combination with a coded destination symbol, the coded designation will be classified at least as high as the meaning of the coded destination symbol. Documents and reports covering shipments may be unclassified where the meaning, coded destination symbols, coded shipment designations, or other coded data covering the shipment are not revealed or otherwise compromised.

e. Movement of personnel or supplies by hospital ship.—Orders for movement of personnel or supplies by hospital ship will be unclassified if it is necessary

SAFEGUARDING MILITARY INFORMATION

AR 380-5
83-87

that such orders accompany the personnel or supplies aboard the hospital ship. See AR 55-530.

84. Dissemination of information.—*a.* All persons connected with the military service who receive information concerning movements of personnel or supplies classified in accordance with paragraphs 83, 90, 91, and 92 are forbidden to make public or to inform unauthorized persons concerning the classified elements of such movements.

b. When it is necessary to advise relatives or other persons of approaching departure, individuals connected with the military service will not disclose any classified information.

c. Arrival in a theater of operations does not diminish the necessity of safeguarding classified elements of information concerning the movement. After such arrival, no information will be given to unauthorized persons concerning names, destinations, or organizations, names of vessels, data concerning convoys, routes pursued, measures taken to avoid attack, date of arrival, debarkation or departure, or number of troops, or kind of cargoes carried.

85. Rail and motor movements.—*a.* Reports concerning arrivals and departure of rail or motor movements within the United States which for any reason are classified, may be transmitted to persons authorized to receive such reports, unclassified, provided unit designations are not included therein.

b. When rail or motor movements or travel of personnel are made preliminary to movement to a theater of operations, cars, baggage, and impedimenta will not be marked in the clear to show oversea destination, date of departure, name of ship, or other classified elements of information. In such cases, impedimenta will be marked with the assigned shipment number and letter or other comparable code designation. The unit designation will not be used as a marking on impedimenta, although the company letter or abbreviation may be used to identify the impedimenta of each company or similar unit in the movement.

86. In staging areas.—*a.* Instructions will be given to all individuals concerned in the applicable security provisions of this section.

b. Commanders of ports or airports of embarkation are authorized to restrict to prescribed limits all personnel under orders for movement to a theater of operations for a period not to exceed 48 hours prior to departure. During this period of restriction, communication with other military personnel and civilians may be prevented or limited as may be considered necessary by the port or airport commander concerned. Special authority must be obtained from the War Department (if in the United States) or the theater commander (if overseas) for placing personnel in restriction more than 48 hours prior to the expected sailing or departure date.

87. Embarkation.—*a.* Troop movements will be made so far as practicable without attracting undue attention. Authority to use bands during embarkation of troops is left to the discretion of port commanders, where, in their opinion, the playing of a band will not jeopardize the security of the movement.

b. All persons not on official business will be excluded from the piers at all times.

c. Personnel may take cameras within the limits of the pier or overseas, subject to the restrictions imposed by the commander of the port, ship, theater, or other area concerned.

d. Members of families, relatives, or friends of personnel under oversea movement or travel orders will not be allowed in the vicinity of piers on the day of sailing.

AR 380-5

88-92

SAFEGUARDING MILITARY INFORMATION

88. Movement of vessels in harbors.—Vessels loaded with personnel or supplies will be moved under cover of darkness whenever possible.

89. At sea.—*a.* After sailing from the port of embarkation, the destination will be disclosed to members of units, replacements, or individuals aboard ship only as necessary for training or indoctrination en route. When such information is disclosed, personnel will be warned of the classification thereof. Particular care will be taken to insure that this warning is given all personnel who are allowed ashore at intermediate stopping points.

b. Events at sea concerning or resulting from enemy action will be considered as secret information by all individuals concerned.

90. Returns to continental United States.—Classification requirements are the same as those enumerated in paragraphs 83 and 91.

91. Movements by air.—*a.* Generally, the same requirements for water movements apply to movements by air of units or subdivisions thereof to a theater of operations.

b. In documents containing information of travel to a theater of operations by military aircraft of replacements, and individuals, as distinguished from units, the inclusion of the following elements normally will require a classification of restricted only:

- (1) Oversea or intertheater geographical destinations, unless the presence of troops or particular military installations at such destinations is classified higher than restricted.
- (2) Date and time of departure from port of aerial embarkation, or airports en route, subsequent to such departure.
- (3) Air route, unless the air route is classified higher than restricted.
- (4) Estimated time of arrival at specific overseas intertheater destination or airports en route, subsequent to departure from port of aerial embarkation.
- (5) Oversea or intertheater destination represented by a temporary APO number.

c. The provisions of paragraph 83 will apply to information concerning the overseas travel of replacements and individuals when both air and water transportation are employed.

d. Orders and allied papers for overseas travel by commercial aircraft of replacements and individuals may be unclassified, even though they contain elements of information for which a classification of restricted is required by *b* (1), (2), (3), and (4) above.

e. All individuals involved in air movements, communicating from intermediate stopping points, will refrain from disclosing classified information.

f. Operational messages limited to information concerning movements of aircraft in a theater of operations may be sent in the clear when authorized by the theater commander.

g. The specific airport of destination within continental United States for returns to the United States by air from theaters of operation is restricted information.

92. Theater of operations in continental United States.—The foregoing paragraphs of this section are based on the assumption that theaters of operations will be located overseas. However, should any portion of continental United States become a theater of operations, the provisions of the foregoing paragraphs nevertheless will apply, subject to the following:

a. The portion so designated will be treated as an "overseas designation."

b. The terms "continental United States" and "United States" will refer only to the zone of interior (see FM 100-5).

SAFEGUARDING MILITARY INFORMATION

AR 380-5
92-95

c. The movements or travel by rail or motor from the zone of interior to the theater of operations, the security provisions applicable to ports of embarkation will also apply to points in the zone of interior from which direct movement to the theater commences, and the provisions applicable to water movement or travel will apply to land movement or travel.

93. Higher classification.—A higher classification than that indicated in this section may be assigned if the order, message, or other communication contains information which should be protected by a higher classification.

94. Reason for classification.—Whenever a classification higher than restricted is assigned to a movement order, the reason for such higher classification will normally be included therein. An *example* of an explanatory paragraph is as follows:

The following secret and confidential elements of information are contained herein: secret equipment (par. 11c); tabulation of units (par 1); confidential mission (pars. 2 and 3). All other elements of this order are restricted.

95. Periods of peace or following termination of hostilities.—a. *Application*.—The provisions of this paragraph will apply only during periods other than those of hostilities.

b. *Normal security requirements*.—Information or documents concerning movement of personnel or supplies will normally be unclassified.

c. *Classification requirements*.

- (1) Elements of information (such as destination, mission, and other elements which should be safeguarded) concerning movements of personnel or supplies, other than movements within oversea areas in which United States Army forces are stationed, will be classified secret, confidential, or restricted only when such classification is authorized by the War Department. Separate instructions directing such classification will be issued to the offices and personnel concerned.
- (2) Commanders of United States Army forces stationed in oversea areas are authorized to classify elements of information concerning movement of personnel or supplies within their respective areas.
- (3) The provisions of paragraphs 84, 85, 86, and 87 will apply to classified movements.
- (4) Whenever a movement order is classified, the reason for such classification will normally be included therein. An example of an explanatory paragraph is as follows:

The following classified elements of information are contained herein. Secret equipment (par 11a); confidential mission (par. 1); restricted consignee combination (pars. 2 and 3). All other elements of this order are unclassified.

[AG 380.01 (2 Aug. 46)]

BY ORDER OF THE SECRETARY OF WAR:

OFFICIAL:
EDWARD F. WITSELL
Major General
The Adjutant General

DWIGHT D. EISENHOWER
Chief of Staff

DISTRIBUTION.

A; E

AGO 385B

43

U. S. GOVERNMENT PRINTING OFFICE: 1946

Unclassified
Serial No. 130

STATE-WAR-NAVY COORDINATING COMMITTEE
SECURITY ADVISORY BOARD
WASHINGTON 25, D. C.

Sec. Regs.

November 7, 1946

MEMORANDUM FOR

State Member, SAB ←
War Member, SAB
Navy Member, SAB

Subject:

Suggested Introduction for Archives Handbook

References:

- a. Serial No. 100
- b. Serial No. 117
- c. Minutes 7th SAB Meeting

Enclosure:

Draft Prepared by Archives Representative

1. Mr. William Ross, representative from the National Archives, is presently reviewing background material on the Security Advisory Board for use in preparing a section on security in the Federal Handbook for Wartime Agencies. He has prepared the enclosed draft as a part of the introduction to the Handbook.

2. The comments and opinions of the Security Advisory Board members are requested.

For the Security Advisory Board:

Ruth C Barton
Ruth C. Barton
Secretary

11-12
Handed
Mrs. Barton

GA

Preliminary draft
October 18, 1946
William F. Ross

(Suggestion for possible statement in introduction to Handbook)

SECURITY AND ACCESSIBILITY OF DOCUMENTS

For reasons of national security, a large number of the records referred to in this Handbook are not available to the public. Most of such records are "classified". Classification is primarily a device for controlling uniformly the security of all copies of a document wherever they may be, and into whatever hands they may fall. It is axiomatic that all copies of a document must bear the same classification. In time of war, a competent official may even classify papers written by private persons or firms, and the classification automatically applies to all copies of such a paper.

There are four classifications: "TOP SECRET", "SECRET", "CONFIDENTIAL", and "RESTRICTED", and the official definitions of each are as follows:

- a) TOP SECRET: Information, the security aspect of which is paramount, and the unauthorized disclosure of which would cause exceptionally grave damage to the nation.
- b) SECRET: Information, the unauthorized disclosure of which would endanger national security, or cause serious injury to the interests or prestige of the nation or any governmental activity thereof.
- c) CONFIDENTIAL: Information, the unauthorized disclosure of which, although not endangering the national security, would be prejudicial to the interests or prestige of the nation, any governmental activity, or an individual, or would cause administrative embarrassment or difficulty.

d) RESTRICTED: Information which should not be published, or communicated to anyone except for official purposes.

From the above, it may be seen that Government employees (including, in some cases, state and municipal employees) may consult RESTRICTED documents. They will in many cases be made available to private scholars whose work is of interest or value to Government agencies, always subject to the rule of "no publication."

Documents within the higher classifications (TOP SECRET, SECRET, CONFIDENTIAL) may be seen only by persons who have received a SECURITY CLEARANCE. Such clearances vary considerably according to the Agency involved and the classification of the documents which it is desired to consult. Application for clearance should be made to the AGENCY SECURITY OFFICER. (A list of Security Officers of Government agencies, with address and telephone extension, is given on page ____).

In addition to "classified" documents, there are other categories of records not available to the public: a) Those under PRESIDENTIAL SEAL may only be seen by permission of the President or his personally appointed deputy. b) Access to documents may be limited or restricted in a number of ways by the head of any Governmental Department or Agency, by simple administrative order. This device is used when the documents circulate only within the Agency which originated them. Permission to see such documents must be obtained from the head of the Agency.

In many cases, it will be found that documents from the same file have been segregated according to "classification." This destroys the continuity of the records, but has great administrative advantages. Any binder, folder, or file must be classified as high as the highest-classified enclosure. As an extreme example, a file of unclassified or RESTRICTED

documents would have to be classified TOP SECRET if one TOP SECRET document were enclosed. Moreover, according to security regulations, the whole file would have to be kept in a combination safe. If the one TOP SECRET document were removed, the rest of the file could be kept simply in a room that was locked when not in use, and would be available, without security clearance, to Government officials.

DECLASSIFICATION

Documents may be declassified or reduced in classification by the same authority that originally classified them, or by higher authority within the same agency. Application to reduce or abolish the classification of a document should be made to the Agency which actually originated that document, which is not necessarily the Agency in whose custody it may now happen to be. Most agencies that have ceased to exist transmitted their functions, as well as their records, to permanent Agencies, and declassification of documents is presumed to be such a function. Declassification, like classification, applies to all existing copies of a document, and notification of such change is made by individual letter, announcement in an Agency journal, or other suitable means. Holders of classified documents will find it very helpful to note such changes on the face of the document itself, giving new classification and authority.

Experience with records of the First World War indicates that most wartime documents decline gradually in significance as they grow older, and that restrictions are relaxed accordingly, the ones most secret being the last to become public property. There have been many exceptions, some of them startling (for example, documents containing the words

"Manhattan Project" passed from TOP SECRET to "UNCLASSIFIED" without intermediate steps). A whole class of exceptions might be found under the heading of Fixed Government Policy. Personnel records are permanently "RESTRICTED" -- even reference to the conduct of specific Civil War veterans is still forbidden. (Naturally, this does not apply to personnel statistics).

An effort is now being made within many agencies to review the security of documents, both specifically and by categories. The policy governing such work, and the progress made, vary greatly from one agency to another, and important changes in the security status of specific groups of records may be expected in the near future. The work would be greatly aided by an overall Government policy and a standard mode of procedure, and these are now under consideration. It is believed that exact information about the security status of specific records will be more valuable if compiled at a later date, and included in finding aids of a more specialized nature. Accordingly no information of this type will be included in this Handbook.

UNITED STATES TARIFF COMMISSION
WASHINGTON

*Sec
Rep.*

May 28, 1947

THE SECRETARY

TO: *Security Advisory Bd.*

*as per telephone
request*

*(Currently effective
sec. regulations in T.C.)*

DECLASSIFIED

UNITED STATES TARIFF COMMISSION
Office of the Secretary

September 25, 1946

OFFICE MEMORANDUM: 7 - 7

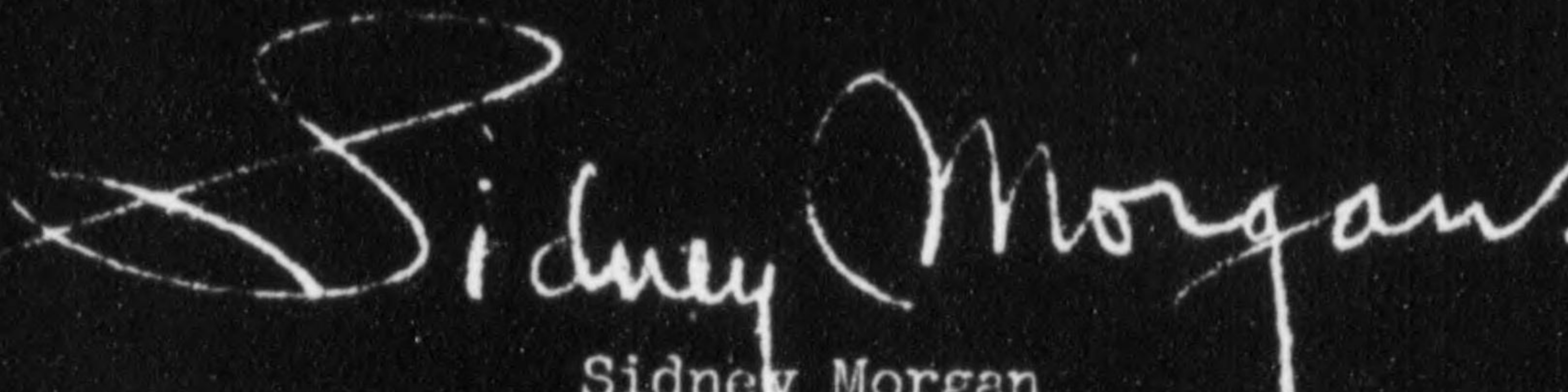
SUBJECT: Peacetime security regulations

The standing rules of the Commission which require confidential treatment of information as to work in progress before the Tariff Commission are repeated at this time to every employee with all possible emphasis.

Controversial matters dealing with commodities and policies are before the Commission and are of the greatest interest to outsiders. Caution is enjoined, therefore, on all employees having knowledge of such matters in order that no disclosures outside the Tariff Commission may occur. The unfinished, unpublicized business of the Tariff Commission is confidential United States Government business and must be safeguarded accordingly. Outside conversations on such subjects with persons not officially concerned are prohibited. Manuscripts and reports dealing with such subjects will be put out of sight and locked away in the most secure file available when the offices are closed.

In accordance with standing instructions (December 18, 1942) draft reports having a confidential character shall be labeled (FOR OFFICIAL GOVERNMENT USE ONLY). This will be followed by such subtitle as the particular circumstances require, for example, "This report includes the costs of individual companies and must not be used or quoted in any manner which will divulge their identities."

Standing instructions with respect to the careful handling, and safeguarding at night and during other periods when the offices are closed, of "SECRET" and "CONFIDENTIAL" material from other Government departments, particularly the military establishments, are repeated for the information of all. Chiefs of services and units will be held responsible for the proper observance of these regulations including the proper clearing of desk tops and work tables at the close of business. Special attention will be paid to security measures in the Graphic Section.

Sidney Morgan
Secretary and Security Officer

*Security Officer File**0.14*

December 18, 1942

MEMORANDUM TO: The Staff.
FROM: The Planning and Reviewing Committee.
SUBJECT: Safeguarding of National Defense Information.

The Office of War Information has recently issued instructions, a copy of which is attached, prescribing that informative material, the improper disclosure of which may have an adverse effect on the war effort, shall be classified as secret, confidential, or restricted. This will directly affect the Tariff Commission in two ways: (1) We must cease the use of "Confidential" in connection with our own more or less regular work, and (2) we must make provision for protecting within our office the material which may be classified as secret, confidential, or restricted under the OWI order.

To put the new procedure into effect, it is proposed that (a) material which we have heretofore marked as "Confidential" shall be labeled "For Official Government Use Only", with such subtitle as the particular circumstances require (for example, "This report includes the costs of individual companies and must not be used or quoted in any manner which will divulge their identities."), and (b) each Chief of Division be required to determine for each job done for a war agency whether it should be classified, and if classified to indicate the lowest category in which it can be placed. Any material classified as secret must be passed upon by the Security Officer, Mr. Whitcomb. Each Chief of Division must undertake to comply with the provisions of the OWI order with respect to the marking, handling, filing, and protection of secret, confidential, and restricted information.

It is the feeling of the Planning and Reviewing Committee that every effort must be made to keep as much as possible of the Tariff Commission's work out of the "Secret" category in order that it may be of more use to the war agencies. This point is very important because secret information has the most limited distribution within the armed forces.

Detailed precautions, varying with the needs in the different divisions handling war information, will need to be adopted. We will be glad to have suggestions from the Chiefs of Divisions in regard to the amplification of this memorandum or clarification of points which are raised in connection with the instructions of the OWI. These suggestions, unless they are too numerous, should be in writing; otherwise, a group meeting can be called to consider them.

E. M. Whitcomb
E. M. Whitcomb,
For the Committee.

(22485)

OFFICE OF WAR INFORMATION

Washington

M-195

September 28, 1942

To the Heads of All Departments and Agencies:

The necessity for a uniform practice within the Government with regard to the security of information has become a matter of some urgency. Practice has differed markedly among the departments, with the result that some documents which should have been treated as secret have been permitted too free a circulation, while others which were in no sense secret or confidential have been improperly classified in these categories.

In order to further uniformity in this regard, I have issued the attached regulations. It is to be noted that these regulations provide only a minimum standard. It would be advisable for each agency to adopt such additional regulations as would:

- a. Make more specific the general regulations of the Office of War Information in accordance with the requirements of the agency; and
- b. Provide for appropriate handling and safeguarding of classified information in accordance with the particular organization and routines of the agency.

I believe that the security of information would be considerably advanced if each agency having classified information were to designate a trusted official as a security officer. May I ask you to be good enough to make such a designation within your own agency?

This Office stands ready to offer such assistance as is possible in facilitating the operations of your security officer.

The Director of the Bureau of the Budget will continue to exercise his responsibilities under Executive Order 9103 in accordance with paragraph 10 a of the enclosed regulations.



Elmer Davis
Director

Enclosures

OFFICE OF WAR INFORMATION

OWI Regulation No. 4

September 28, 1942

TO THE HEADS OF EXECUTIVE DEPARTMENTS,
INDEPENDENT ESTABLISHMENTS, AND OTHER
GOVERNMENT AGENCIES, INCLUDING CORPORATIONS:

In order to provide uniform safeguards over information which might prove of aid or comfort to the enemy and to prevent undue restriction of information which may appropriately be made available to the public, the following regulations are hereby issued by virtue of the authority vested in me by Executive Order 9182.

1. DEFINITIONS

- a. The term "information" as used herein shall include documents, maps, charts, blueprints, photographs, models or other materials which convey information relating to national defense, as well as copies thereof obtained by any means of reproduction or transcription.
- b. The term "classified information" shall designate information relating to national defense requiring special provision for safeguarding. Information which needs no safeguarding shall be referred to as unclassified information.
- c. There shall be three categories of classified information as follows:

Secret Information is information the disclosure of which might endanger national security, or cause serious injury to the interests or prestige of the Nation or any governmental activity thereof.

Confidential Information is information the disclosure of which although not endangering the national security would be prejudicial to the interests or prestige of the Nation or to a governmental activity thereof.

Restricted Information is information the disclosure of which should be limited for reasons of administrative privacy, or is information not classified as confidential because the benefits to be gained by a lower classification, such as permitting wider dissemination where necessary to effect the expeditious accomplishment of a particular project, outweigh the value of the additional security obtainable from the higher classification.

- d. Documents such as books or pamphlets, the pages of which are permanently and securely fastened together, shall receive the most restrictive classification, if any, which is attached to any of the material contained therein.

2. AUTHORITY TO CLASSIFY

The head of each Federal agency or his designated representative shall classify information as secret, confidential, or restricted if the character of the information indicates the need for such classification.

(over)

- 2 -

The authority making the original classification, or superior authority within the agency, may cancel or change the classification of a document, or may direct such cancellation or change.

3. OVERCLASSIFICATION

Documents or materials requiring classification shall be assigned the least restrictive classification consistent with the proper safeguarding of the information or material. Care should be taken to avoid overclassification, particularly in cases where undue restriction may prevent dissemination of information which should properly be disclosed to the public or to Congress.

4. IDENTIFICATION OF CLASSIFIED INFORMATION

a. Classified documents, such as books or pamphlets, the pages of which are permanently and securely fastened together, shall be plainly marked secret, confidential, or restricted on the cover, title page, and first page. Classified communications and other material not permanently and securely fastened together, shall be marked or stamped with the appropriate classification at the top and bottom of each page. The marking at the top shall be so placed that it will not be hidden from view when the pages are clipped or stapled together.

Classified maps and photomaps shall be appropriately marked under the scale.

b. Documents containing classified information furnished persons other than those in the Federal service shall, in addition to being marked secret, confidential, or restricted, bear the following notation:

"This document contains information affecting the national defense of the United States within the meaning of the Espionage Act, 50 U.S.C., 31 and 32, as amended. Its transmission to or the revelation of its contents in any manner to an unauthorized person is prohibited by law."

5. DISSEMINATION OF CLASSIFIED INFORMATION

A. No person is entitled solely by virtue of his office or position to knowledge or possession of classified information. Except as provided by subsections d(3) and d(4) below, such information is entrusted only to those individuals whose official duties require such information.

b. The head of each agency, or his duly authorized representative, shall maintain lists of persons receiving secret information and lists of persons receiving confidential information from that agency.

c. The head of each agency may, by regulation, provide for the registration of secret or confidential information.

d. (1) The distribution of secret matter shall be held to the absolute minimum.

(2) Confidential information shall be disclosed only to those persons in the service of the United States whose duties require that they have such knowledge, except as hereinafter provided.

- 3 -

- (3) Restricted information may be given, when for the good of the Federal service, to any person known to be in that service, provided that the consent of the originating agency is secured; but shall not be released or communicated to the public, the press, or any other agency through which information may be disseminated to the public.
- (4) Under unusual circumstances classified information may be entrusted to persons not in the employ of the Federal Government whose special services to the United States require such information for the more effective rendering of such service, provided that the consent of the originating agency is secured.
- (5) Classified matters shall not be discussed in personal correspondence. Secret matters shall not be discussed over the telephone. Necessary references made to confidential matters over the telephone shall be held to the lowest practicable minimum.
- (6) No secret or confidential information shall be sent in clear over leased or private wire, whether telephone, telegraph or teletype, or in clear over any scrambling device unless the design and installation have been approved by the Signal Corps of the U. S. Army, or other appropriate authority.

6. RESPONSIBILITY

Each agency shall accord to matter classified by any other agency the type and degree of care in handling that is required by the classification marked thereon. The safeguarding of classified information is the responsibility of all employees of the Federal Government. Classified information shall be discussed by persons having access thereto only with other persons authorized to have access to the same information.

7. HANDLING OF CLASSIFIED INFORMATION

- (1) Documents or other materials containing secret information when not in use shall be kept locked in the most secure safe or other container available and in the absence of an authorized employee of the Federal Government, the door or doors of the room in which the safe or other container is located shall also be kept locked.
- (2) Documents or other materials containing confidential information shall be kept in a locked container when not in use.
- (3) Documents or other materials containing restricted information shall be stored and handled in such a manner as to insure a reasonable degree of security.
- (4) Cipher tables, alphabets and keys shall not be kept in the same container as the code books, documents and devices to which they apply.
- (5) In all agencies, appointed officers shall make an inspection immediately before the close of business to insure that all secret documents and cryptographic devices have been properly and safely put away.

- 4 -

- (6) Documents or other materials containing secret or confidential information which are to be transmitted from one person authorized to have such information to another, except when personally delivered by specially authorized personnel, shall be enclosed in an inner and outer cover. The inner cover shall be a sealed wrapper or envelope plainly marked secret or confidential and the outer cover shall be sealed and addressed with no notation to indicate its secret classification. Secret or confidential information when delivered by other than specially authorized personnel shall be transmitted by registered mail. Restricted information may be delivered by any authorized messenger or transmitted by ordinary mail. In no case shall the outside envelope indicate the classified nature of the contents.
- (7) Upon direction of competent authority, classified information shall be destroyed in such a fashion as to render it useless and to prevent any possibility of its falling into the hands of an unauthorized person.
- Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, and work sheets containing classified data shall be destroyed by the person responsible for their production immediately after they have served their purpose or shall be given the same classification and safeguarded in the same manner as the material produced from them.
- (8) Special procedures shall be instituted by each agency in mail rooms and in duplicating and tabulating units which will insure handling of secret and confidential information only by specially authorized employees.
- (9) Each agency sending or receiving secret or confidential messages in code or cipher shall appoint a cryptographic security officer who shall be the custodian of cryptographic material and shall be responsible for all measures necessary to insure cryptographic security under appropriate regulations issued by the head of the agency.

8. REGULATIONS TO BE ISSUED

The head of each agency shall issue such further regulations as he may deem necessary to enforce the provisions of this order and shall assume responsibility for its enforcement.

9. ESPIONAGE ACT

Attention is directed to the following extract from the Espionage Act concerning unlawful disclosures of military information through willful action or gross negligence:

"Whoever ... being intrusted with any document ... relating to the national defense, willfully communicates ... the same to any person not entitled to receive it, or willfully ... fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or ... through gross negligence permits the same to be removed from its proper place of custody ... shall be punished by imprisonment for not more than ten years and may, in the discretion of the court, be fined not more than \$10,000."

- 5 -

10. EFFECT AND DURATION

- a. Subject to these regulations and such further regulations as may be issued by the Director of the Office of War Information, the classification and publication of statistical information shall be in accordance with determinations made by the Director of the Bureau of the Budget as provided in Executive Order 9103.
- b. These regulations shall take effect immediately and shall remain in effect until further notice.



Elmer Davis
Director

Sec Regs.

UNCLASSIFIED
Serial No. 40
ERC/lsh

17 June 1946

MEMORANDUM FOR Mr. John S. Lucas, Security Officer
Department of Agriculture

Subject: Guide for the Disposal or Declassification of
Classified Records

Enclosure: Proposed Memorandum on Subject to be Issued by the
Department of Agriculture

1. Pursuant to our conversation 13 June 1946, your proposed memorandum regarding the disposal and declassification of classified records was submitted to the Security Advisory Board for their approval at their 3rd Meeting 14 June 1946.

2. It was the opinion of the Security Advisory Board that classified reference material which is no longer of value to your department and does not form an integral part of your records could not be destroyed without the required record-keeping set forth in paragraph 9 b of SAB No. 1. At the direction of the Board, alternative paragraphs to incorporate provisions for the required certifications on destruction of classified material have been prepared and are enclosed for your consideration.

3. Such other changes in wording as are indicated in the enclosure were suggested by the Board members and do not change the substance of your memorandum. According to the agreement reached in our telephone conversation 14 June 1946, paragraph (3) of your memorandum has been omitted.

4. It is requested that the Security Advisory Board be provided with a copy of this memorandum when issued.

For the Security Advisory Board:

M. RUTH CATLETT
Capt., WAC
Secretary

ENCLOSUREDECLASSIFICATION AND DISPOSITION OF SECURITY
CLASSIFIED (TOP SECRET, SECRET, CONFIDENTIAL
AND RESTRICTED) DOCUMENTS

A number of inquiries have been received in this office regarding the procedure to be followed in declassifying and disposing of classified material. It is suggested that the following be used as a guide when disposing of or declassifying classified records.

1. Material classified as Top Secret, Secret, Confidential, or Restricted falls into two categories:

a. Material originating in your office which you have the authority to declassify, provided it does not contain information of a military nature.

b. Material originating outside your office or outside of the Department, which you do not have the authority to declassify until permission is obtained from the source.

2. Classified records may be disposed of or declassified according to the following rules:

a. When classified reference material from another source is no longer of any value nor is an integral part of the important records, it can be burned upon direction from a competent authority, or returned to the originating agency.

(1) Classified material which is to be disposed of must be burned and should under no circumstances be placed in ordinary trash receptacles for disposition.

(2) Classified material should be burned by the custodian thereof in the presence of a disinterested official. A certificate of destruction will be signed by both the custodian and the witnessing official in the case of Top Secret and Secret documents or registered publications and submitted to the authority directing the destruction. Where the custodian and the authority directing the destruction are the same, the certificate of destruction will be filed in the office of the custodian of the classified material, where it will be available for reference and/or inspection.

(3) No certificate of destruction will be required in the case of confidential or restricted documents, destroyed under provisions of paragraph 1 above.

b. When it is desired to declassify or downgrade classified material from some other source, not covered by the definition in paragraph 1 above, approval of a request for such declassification or downgrading must be received from the originating office prior to change or cancellation of classification.



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
OF
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.

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:

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 (OCL) 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

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
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)

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.

C. 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 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.

6. 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* envelope, 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 Pouch facilities.

(2) CONFIDENTIAL material for transmission via Diplomatic Pouch 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.

(1-1-47)

(TL 39)

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).

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

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.

201.1

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	VIIIA, B, C2, 3; XB2
to classified material	XIIIF1, 2
to Code Room	IVB2
Accumulated Files	
Additional safeguards, for transmitting	VIIIB
Top Secret Material	XIIIA4
Address, in classified telegrams	VIIIB1b (3), c (1),
Addressing, classified material	(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	VIIB2
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. ICl, XB3,8, XIA

Careless talk. VIB

Certification for access to
Top Secret. VIIIB1e(2)

Classified Material

 changing classification of. IVB

 custody IXA

 definition. ICl

 Destruction, disposal XIB

 dissemination and distribution. VA3, VID, VII

 downgrading and declassifying
 extracts from IIF, IVB

 knowledge of. IIB

 marking of. VIIA

 of defunct Agencies VB, C

 of foreign Agencies IVB4

 of other Agencies IIG, IVB3

 outside of storage place. IIG, IVB4, VA4, VIID2

 possession of IXB

 preparation of. VIIA

 protection of VA, XB4

 publication of. ICl4, VI

 removal from Dept. VIC

 reproduction of IXC

 requests for. VA

 responsibility for. VIIB2, VIID1,3

 return of to Dept. VIA, XA, B, C,

 review of assigned classifications. IXC5

 right to receive. IVA4

 safeguards. VIIB

 stencils. XB, C

 storage XB8

 telegrams ICl4, IXB, XC

 tissue sheet copies XIIIIA

 transmission of XB8

Collection Points, for classified waste. VIIIB

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, XIIIIA7, XIIIIB4

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	XIIIF7
definition	IC5
protection of	XIIID, F
Custodian	
of classified materials	IXA
of cryptographic materials	XIIIIG3
Custody	
of Secret, Confidential, Restricted material	IXA
of keys	IXB7, D
of Top Secret material	VIIIIB1a(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	VIIIIB2c(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	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. 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

- O -

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

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

- S -

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), 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

- T -

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 VIIIIBle
Classification procedure. IVAL
Control Officer VIIIIBle, IXC
definition and examples IIIA
destruction, disposal of. XIB
distribution outside Department
handling. VIIC, D, VIIIIBld
marking VIIC, VIIIIB1, XB, C
protection of VC3, VIIIIB1
storage IXA, XB
testimony IXB1, 5
VIF2

Transmitting, transmission, of
classified material VIII, XIIIC, F3
between organizational units. VIIIIB1b, 2a, 3a, 4a

Security Messenger Service (see Security Messenger
Service)

confidential material VIIIIB3
outside Department. VIIIIBld, 2c, 3c, 4c
restricted material VIIIIB4
secret material VIIIIB2
to Foreign Service Post VIIIIB1c, 2b, 3b, 4b
to other Government Agencies. VIID, VIIIIBld, 2c,
3c, 4c,
Top Secret material VIIIIB1
via Diplomatic Courier. VIIIIB1c (4), 2a (4),
b (4)
via regular Messenger Service VIIIIB2, 3a, 4a, c
via responsible personnel VIIIIB1a (1), b (1), (2),
(4), 2a (1), (2), (4),
3a (1), 4a
within Foreign Service. VIIIIB1b, 2a, 3a, 4a

- U -

Unclassified material, information
marking IIA
telegrams IIIIE, 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