THE JOINT RESEARCH AND DEVELOPMENT BOARD

SECURITY REGULATIONS

15 JUNE 1947

ADMINISTRATIVE SERIES NO.1

JRDB 74/1

ADMINISTRATIVE SERIES No. 1
JRDB 74/1 15 June 1947

SECURITY REGULATIONS

THE JOINT RESEARCH AND DEVELOPMENT BOARD
of the War and Navy Departments
Washington 25, D. C.

Prepared by the
PROGRAMS DIVISION
and the SECURITY OFFICE

Approved by: E. W. Richardson
Administrative
Secretary

FOREWORD

The official security regulations governing the production, dissemination, distribution, and handling of classified information by all personnel of the Joint Research and Development Board and its agencies are hereby promulgated in accordance with Section 6.2 of the Rules of Organization and Procedure, which directs that "The Executive Secretary shall issue the security regulations of the Board to effectuate the U. S. Codes and Statutes relating to security of information."

L. V. BERKNER
Executive Secretary

June 15, 1947

SECURITY REGULATIONS OF THE JRDB

TABLE OF CONTENTS

6/15/47

3.5 Security Measures for Individual Offices

3.5.1 The Issuance of Keys

3.5.2 Protection Against Unauthorized Inspection

3.5.3 Security of Desks, Safes, and File Cabinets

3.5.4 Attendance in Office

3.5.5 Disposition of Office Waste Material

3.5.6 Stowage and Filing of Classified Documents

3.5.6.1 Top Secret Material

3.5.6.2 Secret and Confidential Material

3.5.6.3 Restricted Material

3.6 The Preparation of Classified Correspondence

3.6.1 Securing Log Numbers for Top Secret and Secret Correspondence

3.6.2 Number and Colors of Copies for Correspondence Below Top Secret

3.6.3 Number and Colors of Copies for Top Secret Correspondence

3.6.4 Affixing the Classification and Espionage Act Stamps

3.6.5 The Preparation of Receipts

3.6.6 The Preparation of Envelopes for Classified Correspondence

3.6.7 The Destruction of Waste Materials

3.7 The Transmission of Classified Documents

3.7.1 Inter-Office Transmission

3.7.1.1 Top Secret

3.7.1.2 Secret

3.7.1.3 Confidential and Restricted

6/15/47

6/15/47

SECURITY REGULATIONS OF THE JRDB

Most of the information with which the JRDB is dealing in its daily work is vital to the defense of the United States. Such information is known as "classified information" and has been graded to indicate the degree of its importance into Top Secret, Secret, Confidential and Restricted. In order to safeguard the classified information in its possession, the Board has established a series of security regulations which are set forth in this chapter and has evolved certain specific procedures for the handling of classified information. It is incumbent upon every member of the staff, regardless of the position he holds, to be thoroughly conversant with these regulations and procedures and to observe them to the letter. Breaches of security may not be excused by "ignorance of the law."

The Joint Research and Development Board is necessarily high on the list of targets for unauthorized persons who desire to obtain information regarding the national defense. Such persons are shrewd and determined and will seek to gain their ends by clever and indirect means. No security system is perfect nor secure against such efforts, unless each person who knows any part of the desired information is on his guard at all times. This means that members of the staff must guard particularly against discussing office business with relatives or friends. Since the smallest and most irrelevant fact may be

6/15/47

significant if it falls into the hands of those who can associate it with other facts, the only safe rule to follow is not to discuss any office business outside the office.

3.1 Personal Responsibility of the Individual.

Each person, regardless of capacity in which he may receive it, becomes personally responsible for classified information with which he is entrusted. Executive Directors of Committees and other officials of the Board are responsible for acquainting all personnel under their direction with the security regulations and for seeing that the rules of security are fully met with respect to their own offices. New personnel should be so indoctrinated as soon as they enter on duty. Knowledge of classified information should be limited to those who require such knowledge for the discharge of their duties. Work for clerical personnel shall be arranged in such a way that one person will work on the same paper from beginning to end in so far as possible. Each individual is personally accountable, however, for the security of all information which he receives in his official capacity.

3.1.1 Penalties for Violation: All loyal citizens who have the welfare of their country at heart, will naturally exercise the greatest diligence in safeguarding information which affects the national defense. It is necessary to point

out, however, the law provides heavy penalties for those who violate their trust. JRDB personnel entering on duty for the first time are required to read and understand the Espionage Act /The Act of June 15, 1917, 40 Stat. 217 as amended by Section I of the Act of March 28, 1940, 54 Stat. 79, 50 USC 31 (Fine and Imprisonment for Disclosure of Information) and Executive Order #8381 of March 22, 1940/ "defining certain vital military and Naval installations and equipment." It goes without saying, of course, that the Executive Secretary has heavy responsibilities for the security of information within the Board. The necessity for exercising the utmost diligence in this respect outweighs any personal considerations, and any lapses from security will be dealt with stringently and without regard to the personalities involved.

3.1.2 The Oath of Secrecy: All JRDB personnel entering on duty for the first time are also required to read and sign the Oath of Secrecy, text of which is as follows:

OATH OF SECRECY

I, the undersigned, ... do solemnly swear or affirm that, in consideration of the purpose and aim of JRDB in coordinating scientific knowledge and information, that whenever I receive classified information, orally or in writing, pertinent to the national defense, security, and welfare of the United States:

3.1.2(2)

1. I will neither supply nor disclose to any unauthorized person any classified information which is disclosed to me in any manner in connection with my official capacity with the JRDB, and I further agree not to disclose to any unauthorized person the Board's interest in any field of scientific research or development unless such disclosure is previously approved by the Executive Secretary of JRDB or his representative.

2. I will not duplicate, or cause to be duplicated by either printing or other reproductive processes, any JRDB TOP SECRET, SECRET, or CONFIDENTIAL material which has been made available to me; unless prior approval for such reproduction has been granted by the Executive Secretary, his Deputy, or other authorized person.

3. Upon completion of my connections with JRDB, I will promptly return all classified material for which I assumed responsibility while under the jurisdiction of the Board.

4. I have read and understand the attached copies of the following acts:

   a. Espionage Act: See 1d. and e. of the Act of June 15, 1917, 40 Stat. 217, as amended by Sec. 1 of the Act of March 28, 1940, 54 Stat. 79, 50 USC 31 (Fine and imprisonment for disclosure of information) (Incl. 1).

   b. Executive Order No. 8381 of March 22, 1940, 5 F. R. 1147 (Incl. 2).

So help me God:

____
(Signature)

Witness:

____

____

6/15/47

New personnel are required to report to the Security Office upon arrival and to read and initial the copy of the Security Regulations held by the Security Office within 72 hours after their arrival.

3.1.3 Personnel Investigations: One of the primary precautionary measures taken with respect to safeguarding classified information is the investigation through the investigative facilities of the government, of all personnel who enter on duty with the Board. This practice, which has recently been made mandatory for the Federal Service by Executive Order, has long been a requirement in the War and Navy Departments and other Agencies handling highly classified information. Each person is required to furnish certain basic data regarding his own personal history which is used by the investigative agencies to facilitate their inquiries. Persons on whom no derogatory information is found are unofficially referred to as having been "cleared." It is emphasized, however, that notice to the effect that clearance has been given may signify only that the investigation has been made and no evidence uncovered to indicate that the person is disloyal or untrustworthy. It does not mean that any and all classified information may be given to that person indiscriminately. Each individual is entitled to only such classified information as he

requires for the performance of his official duties. The Executive Secretary has delegated to the Administrative Secretary the authority to decide what level of classified information may be handled by each employee. The Security Officer will convey this information to the employee's supervisor.

Persons who by virtue of their official positions are entitled to an overall knowledge of classified information, should exercise the greatest diligence and discrimination in passing on portions of that information to their subordinates. If a person must be used in handling classified material before he is cleared, authorization must be obtained from the Security Officer.

3.1.4 Obligations Upon Leaving the JRDB: Persons leaving the JRDB on any basis whatever--separation, transfer, resignation, etc.--may not disclose, after leaving, the classified information which they received while associated with the JRDB. Further, each person leaving the JRDB is required to return all official documents, classified and unclassified, identification passes, keys, etc., and will be required to sign a statement that no such material or equipment remains in his possession.

3.2 Definitions of Terms in Commonest Use.

The purpose of this section is to define the security terms in most general use in order that there may be a common understanding regarding them throughout the Board. The definitions have, for the most part, been taken from the Army Security Regulations[1] or the Navy Security Regulations[2].

Classified Military Information: Includes all information concerning documents, cryptographic devices, development projects and materiel falling in the categories Top Secret, Secret, Confidential, or Restricted.

Confidential Matter: Documents, information, or materiel, the unauthorized disclosure of which, while not endangering the national security, would be prejudicial to the interest or prestige of the nation, any governmental activity, an individual, or would cause administrative embarrassment or dificulty, or be of advantage to a foreign nation.

Cryptographic Material: Includes all documents and devices employed in changing plain language messages into unintelligible form by means of codes and ciphers.

Documents: Any form of recorded information, such as printed, mimeographed, typed, photostated, and written matter of all kinds;

1 Safeguarding Military Information (Army Regulations 380-5), 15 August 1946.
2 Procedure for Safeguarding Top Secret Matter and Article 76, U. S. Navy Regulations, 1920.

charts, maps, relief maps, photomaps, and aerial photographs and mosaics; drawings, sketches, notes, and blueprints, or photostatic copies thereof; photographs and photographic negatives; recorded engineering data; correspondence and plans relating to research and development projects; and all other similar matter.

Materiel: Any article, substance or apparatus. The term materiel comprises military arms, armament, equipment, and supplies of all classes, both complete and in process of development and construction, models that show features in whole or in part, design, mock-ups, jigs, fixtures, and dies, and all other components or accessories of military equipment.

Officer Courier: Commissioned officers of the Army, Navy, Marine Corps, and Coast Guard on active duty and commissioned officers of the Naval Reserve, Marine Corps Reserve, and Coast Guard Reserve on active duty.

Photomap: A reproduction of a photograph or mosaic upon which grid lines, marginal data, and place names may be added.

Registered Documents: Any document or device registered usually by number and periodically accounted for. A registered document is a Top Secret, Secret, or Confidential document, or a Restricted cryptographic document, or device, carrying a register number, a short title, and instructions to account for it periodically. A registered document is not to be confused with a classified document to which, for administrative reasons, a number or short

title is assigned for bookkeeping or reference purpose only, and for which no accounting is required.

Restricted Matter: Documents, information, or materiel (other than Top Secret, Secret, or Confidential) which should not be published or communicated to anyone except for official purposes.

Secret Matter: Documents, information, or materiel, the unauthorized disclosure of which would endanger national security, cause serious injury to the interests or prestige of the nation, or any governmental activity thereof, or would be of great advantage to a foreign nation.

Short Title: A designation applied to a classified document, materiel, or device for purposes of security and brevity. It consists of figures, letters, words, or combinations thereof, and if registered usually contains an abbreviated designation of the office of origin, without giving any information relative to classification or content of the document, materiel, or device.

Technical Information: Shall be deemed to include information on weapons and equipment, including instructions on maintenance and operation and any descriptive matter on components. It further includes means of manufacture, techniques, and processes of weapons and equipment, together with information pertaining to the various sciences relating to weapons and equipment and to direct and indirect measures which may be employed in warfare. Information of a strategic or tactical nature is specifically

excluded from the meaning of this term as are "user" aspects such as functioning and general instructions for tactical use and employment.

Top Secret Matter: Certain secret documents, information, and materiel the security aspect of which is paramount, and the unauthorized disclosure of which would cause exceptionally grave damage to the nation.

3.3 Security Office.

The responsibility for the administration of security within the JRDB rests with the Administrative Secretary under whose supervision the Security Office is established and maintained.

3.3.1 Military Personnel in Charge: An officer of the Army or the Navy acts as Security Officer in the Joint Research and Development Board. An officer from each Service is assigned to the Security Office and one of them is on duty at all times during the working day.

3.3.2 Hours of Duty: The Security Office will open not later than 0800 and will close not earlier than 1730. A Security Officer will be on duty at all times during these hours. If it becomes necessary in emergency situations for both Security Officers to be absent from the Security Office at the same time, the office will be supervised by

a civilian employee properly cleared and specifically authorized by the Administrative Secretary. If it is necessary for any personnel of the Board to work after 1730, the Security Officer making the nightly check will notify the working staff that it is responsible for securing the offices used, which includes stowing all classified material in safes commensurate with their security and locking the office doors.

If it is necessary for personnel to work Saturdays or Sundays, the same rules will apply.

A Security Officer will be in attendance at all meetings of the Board, the Policy Council, the Scientific Advisors to the Policy Council, and the Executive Council, whenever such meetings are held outside regular working hours or outside the official headquarters of the Board.

3.3.3 Authority: The Security Office of the Board is the authorized representative of the Executive Secretary, and all orders and instructions from the Security Officer with respect to security have the same authority as though emanating from him.

3.3.4 Responsibilities: The Security Officer is responsible for the following matters:

(1) The internal security of the building area occupied by the Board.

(2) Approval of all Security Regulations issued by the JRDB.

(3) The maintenance of order, enforcing the Security Regulations, and making security inspections.

(4) Instruction of personnel in the Security Regulations and procedures at JRDB.

(5) The receipt, logging in, and distribution within the JRDB of Top Secret material.

(6) Distribution of Top Secret material by officer courier or other designated courier.

(7) The safeguarding of Secret and Top Secret documents which are forwarded to this office or which originate in this office; under no circumstances will Top Secret or Secret material repose in a Committee file until registered with the Security Officer.

(8) The destruction of classified material. A report of the destruction of classified material prepared by the JRDB will be made to the Executive Secretary and filed in the Security Office. If classified documents of a headquarters other than the JRDB are destroyed, the Security Officer will notify the issuing headquarters of the destruction. (It is the

responsibility of the Management Division to effectuate the daily collection and burning of classified papers.)

(9) The survey at intervals not exceeding three months, of all classified material on file with the Board.

(10) Reporting to the Administrative Secretary and the Executive Secretary, all security violations without exception, discovered during the day or during the nightly check of the offices.

(11) Changing combination locks at least once every 6 months, or upon separation from the office of personnel who have knowledge of the combination, except that the combination to the main vault shall be changed at irregular intervals not to exceed 30 days.

(12) The custody of lost and found articles. Inquiries for lost items should be made to the Security Officer.

3.4 Rules for Admittance to JRDB Premises.

All persons entering the premises of the JRDB will be admitted only upon the display of proper credentials and satisfactory personal identification. A receptionist will be on duty at all times during the working day to attend to the details of admittance and exit.

6/15/47

3.4.1 JRDB Personnel: All personnel of the JRDB including the Army and Navy personnel, regular full-time personnel, part-time consultants and technical advisors are required to display the JRDB pass.

3.4.2 Visitors: Upon the arrival of a visitor, the receptionist will telephone the office of the person to be visited; if that person is in, the visitor will be asked to wait in the ante-room until the person upon whom he is calling comes to meet him or sends someone to do so. If the caller is not to be met and escorted, then it is necessary for the visitor to sign in at the reception desk. It is necessary that the reception desk have a record of all visitors, and JRDB personnel who bring visitors in with them are requested to leave information regarding the visitors with the receptionist. In the event they fail to do so, the receptionist will call for this information. All visitors are required to display personal identification.

3.4.3 Telephone Company or Building Employees for Service Purposes: Chesapeake and Potomac Telephone Company employees and Government service employees will show photographic identification signed by either the Provost Marshal, or by an authorized representative of the Navy Department. The receptionist shall direct to the Security

Officer all employees admitted to the premises of the Board for service purposes. The Security Officer will ascertain the areas in which they work and will notify the offices involved of their presence. These offices will take the precautions necessary to avoid breach of security.

Commercial deliveries may not be made within the premises of the Board, but in emergency situations may be left with the receptionist who will notify the addressee.

3.4.4 Admittance to Conferences: The only persons permitted to enter a conference room during a meeting are members of the Secretariat. Persons desiring to deliver a communication to a conferee will turn it over to the receptionist or to the Executive Secretary's secretary who will be responsible for its delivery.

3.4.5 Property Inspection and Clearance: Visitors to offices of the Board who carry brief cases, envelopes, or parcels should request from the receptionist or authorized person in the office visited, a signed Property Pass which will enable the visitor to leave the building without detailed inspection by the building guards. A list of personnel authorized to sign Property Passes is attached as Appendix I of this chapter.

3.5 Security Measures for Individual Offices.

The security of the individual office is the responsibility of the head of the office. It shall be his duty to ascertain that all personnel under his supervision are thoroughly acquainted with JRDB security regulations and cognizant of their personal responsibilities in the matter of security. Any breaches of security which occur within an office shall be charged against the head of the office.

3.5.1 The Issuance of Keys: Office keys shall be issued to the head of any office of JRDB upon his request. Keys may be issued to subordinates in any office upon certification by the head of the office, to the Security Officer, that the possession of the key is necessary to the effective conduct of the work in that office. Issuance of keys shall be kept to a minimum consistent with effective conduct of JRDB business.

Keys to desks are supplied by the Supply Section of JRDB and are issued to individuals by that section. Upon delivery of desk keys to individuals, a signature is obtained for the key and filed with the Security Office. It is necessary that people upon changing desks notify the

Security Office of this change so that the records may be altered.

Keys will not be issued to any individual when changing desks unless the old key is returned to the Security Office and the exchange of desks reported.

3.5.2 Protection Against Unauthorized Inspection: Persons having classified information on their desks will take every precaution against unauthorized persons inspecting such material either deliberately or casually. One precautionary measure is to keep such papers face down or covered when not in immediate use; another is to provide a conference table where officers of the Board may interview guests rather than at their desks where classified papers may be in use.

3.5.3 Security of Desks, Safes, and File Cabinets: All classified papers must be stowed in accordance with security measures appropriate to their classification (Section 3.5.5) at night and during any periods of the day in which the office is unattended.

When cabinets and safes are unlocked, a "T" shaped card with the word "OPEN" on it shall be inserted in the handle

of the top drawer. These cards shall be removed only when the safes and cabinets have been secured.

All personnel who have been entrusted with the responsibility for securing safes and cabinets should be thoroughly familiar with the operation of the combination locks. There have been instances where the custodians of classified material have unwittingly left safes, safe cabinets, and file cabinets unlocked because of their unfamiliarity with the combination locks. Persons charged with the locking of safes and cabinets should make certain that each drawer and compartment is in position before turning the dial. The dial should be turned at least three complete revolutions and the cabinet or safe checked thereafter to insure that the lock has functioned. Army and Navy regulations require that the combinations of lock type safes and cabinets be changed periodically. It is desired that combinations of all safes be changed:

(1) at least every six months;

(2) upon permanent detachment from the office of any personnel having knowledge of the combination. Combinations on all safes must have a final number not lower than 15.

3.5.4 Attendance in Office: At no time may an office be left unattended while classified papers are lying about and safes and cabinets open. Whenever an office must be left unattended, it shall be secured in the same manner as at the close of the business day.

Between the hours of 1700 and 0830, except when attended, all offices will be entirely cleared of loose papers, calendars, telephone lists, any written materials or documents; and all such materials and documents shall be properly stowed. All written materials or documents, including unclassified materials must be placed under lock and key to ensure that no classified material is inadvertently left exposed. Certain exceptions to this order are permissible:

(1) Supplies, which may be stored in unlocked cabinets or other repositories which permit ready inspection when these are neatly stacked to indicate clearly that no written or printed documents are inadvertently stored with them;

(2) Unclassified reference information regularly posted on walls or desks;

(3) Restricted information regularly posted, with the authorization of the Security Officer.

Windows should be secured when the last member of the staff of an office is leaving for the day.

3.5.5 Disposition of Office Waste Material: All classified waste office material must be placed in the wastepaper baskets marked SECRET. A supply of these is in each office. Classified waste office material should be torn into small pieces before being deposited in the SECRET baskets. Under no circumstances should it be burned in the receptacles.

All non-classified waste papers and other trash should be deposited in the receptacles provided in the halls for this purpose and not deposited in the SECRET receptacles. Contents of wastepaper baskets will be collected daily between 1600 and 1645 by the messenger. When wastepaper baskets are emptied, they will be turned upside down. Under no circumstances will classified materials be placed in the wastepaper basket after the waste collection has been made.

3.5.6 Stowage and Filing of Classified Documents: Classified documents must be stored under security conditions commensurate with their classification, outlined as follows:

3.5.6.1 Top Secret Material: Top Secret documents shall be stored by the Security Officer in a six-combination safe. Under no circumstances may Top Secret documents be stored elsewhere.

3.5.6.2 Secret and Confidential Material: Secret and Confidential material must be secured in a three-combination safe or in steel cabinets secured by bars and three-combination locks. Secret and Confidential material may be stored within the offices to which it belongs or where it is being used. Secret route sheets will not be filed with secret material other than in the central files. If a Committee or Panel desires to file secret material, it will so indicate on the route sheet, initial the route sheet, and return it to central files through the Security Office.

3.5.6.3 Restricted Material: Restricted documents may be kept in desks provided the desks are locked. Restricted documents not kept in a locked desk will be secured in the same manner as confidential documents. Restricted material, provided it bears the Security Officer's notation of approval, may be posted in rooms normally kept locked after

business hours. Restricted documents may be filed in the offices to which they belong or in which they are being used.

3.6 The Preparation of Classified Correspondence.

(NOTE: The preparation of correspondence generally is covered fully in Chapter 6, Mail and Correspondence. The purpose of this section is to spell out the rules which apply to the preparation of classified correspondence.)

All classified correspondence shall be prepared and dispatched in accordance with this Section. Responsibility for the proper classification of outgoing classified correspondence rests with the originator.

3.6.1 Securing Log Numbers for Top Secret and Secret Correspondence: Any office preparing Top Secret correspondence must send a secretary to the Security Officer to apprise him of the fact and to secure from him a log number. The secretary shall, at the same time, advise the Security Officer of the number of copies to be prepared and the proposed distribution. Offices preparing Secret correspondence shall contact the mail control desk and request log numbers for each piece of secret correspondence. The mail control

clerk will make a pencil note of the log number. The secretary preparing the Secret correspondence will type the log number on the upper righthand corner of the correspondence. When the correspondence is received in the Mail Room, the mail control clerk will make a permanent record of the number in ink.

3.6.2 Number and Colors of Copies for Correspondence Below Top Secret: For classified correspondence below Top Secret, a route sheet should be prepared. Route sheets are colored and labeled, according to classification, as follows: Restricted, green; Confidential, yellow; Secret, blue. The following carbon copies of the letter should be made: original, three white copies, one green copy, one pink copy.

3.6.3 Number and Colors of Copies for Top Secret Correspondence: For Top Secret Correspondence, a pink route sheet should be attached, and the following carbon copies of the letter prepared: original, two white copies, one green copy.

3.6.4 Affixing the Classification and Espionage Act Stamps: All classified correspondence must be stamped at the top and the bottom of each page with the appropriate classification stamp. The top marking must be placed in such

a way that it will not be obscured by paper clips, staples, or file fasteners. All classified correspondence addressed to a civilian agency, or which may be forwarded to a civilian agency, must bear, in addition to the security classification, the following reference to the Espionage Act:

> This document contains information affecting the national defense of the United States within the meaning of the Espionage Act (U.S.C. 50:31 32). The transmission of this document or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

Rubber stamps for the security markings and the Espionage Act reference may be secured from the Supply Section of the Management Division.

3.6.5 The Preparation of Receipts: The preparation of receipts is mandatory for Top Secret and Secret material. The preparation of receipts for Confidential matter is optional with the office of origin.

Receipts for Top Secret correspondence will be prepared by the Security Office, which should be notified when Top Secret documents are ready for transmittal.

Receipts for Secret material (W.D., AGO Form No. 996) should be prepared in accordance with the following

procedure by the offices originating the correspondence: Receipt forms may be procured from the Security Office, the mail control desk, or the Supply Section. Receipt forms shall be made in triplicate. The standard forms in use come made up in three copies. The secretary completing the receipt shall fill in (1) the date of the correspondence; (2) the space labeled "Serial No., File No. or Subject" as follows: the first letter of the classification--the log number--and the copy numbers; (3) the log numbers of any Secret enclosures (if classified; otherwise, the number of enclosures); (4) the addressee as appropriate. If there are no enclosures, that part of the form should remain blank. The Postal Registry number will be filled in by the Mail Room. Under no circumstances should classified information be included on the Receipt Form.

Receipt forms should be enclosed in the inner envelope which, together with the outer envelope, should be delivered unsealed to the Mail Room.

3.6.6 The Preparation of Envelopes for Classified Correspondence: Restricted correspondence may be forwarded in a single opaque sealed envelope. No indication of classification should appear on the envelope. An inner and an outer envelope must be prepared for Confidential, Secret, and

Top Secret correspondence. The inner envelope shall be smaller than the outer, stamped with the appropriate classification stamp, and addressed in a manner identical with that of the outer envelope. Classified correspondence should be addressed only to persons or desks known to be authorized to receive classified correspondence.
The outer envelope should be opaque, larger than the inner one. Lined letterhead envelopes may be obtained from Supply Room. The outer envelope should bear no indication of classification.

3.6.7 The Destruction of Waste Materials: All waste materials resulting from the preparation of classified correspondence must be destroyed. These include carbon paper, rough drafts, and stenographic notes, when they have served their purpose. Such matter should not be left in desks over night. The Security Office shall destroy all waste material for Top Secret correspondence.

3.7 The Transmission of Classified Documents.

Classified documents may be transmitted only in accordance with the procedures prescribed in this Section.

3.7.1 Inter-Office Transmission:

3.7.1.1 Top Secret.* Top Secret documents, in folders, will be transmitted between offices by the Security Officer only. Under no circumstances shall Top Secret material be sent through the inter-office mail. Top Secret material should not be removed from its folder. All Top Secret documents brought into the Board from any source must be logged in at the Security Office before being put to use.

3.7.1.2 Secret: Secret documents, in folders, will be transmitted between offices by members of the Security Office only. Secret material should not be removed from its folder. Secret incoming material will be forwarded to the Security Office from the mail control desk. The Security Office will be responsible for the distribution of all Secret material until such material is placed in file. Secret material in file which is to be rerouted to interested committees, panels or persons will be routed through the Security Office.

* Members of the staff of the Board authorized to handle Top Secret material are listed in Appendix II to this chapter, copy of which may be seen in the Security Office.

3.7.1.2(2)

Requests for Secret documents that have been filed in the Library will be handled in the following manner: the request will be made to the Librarian who, upon extracting the document from the file, will attach the appropriate route sheet and indicate on the route sheet the log number and the addressee. The document will then be forwarded to the Security Office by folder, and there it will be distributed to the requesting office. After the requesting office has finished with the document and initialed the route sheet, it will be returned to the Library by way of the Security Office.

Secret and Top Secret material will be delivered in folders by the Security Office. These folders will be delivered daily not later than 1000 and will be picked up by a representative of the Security Office in the afternoon. The representative of the Security Office will start picking up folders at 1530. NO SECRET OR MATERIAL OF HIGHER CLASSIFICATION IS TO BE TAKEN FROM THE JRDB OFFICES BY ANY PERSONNEL WITHOUT CLEARANCE THROUGH THE SECURITY OFFICE.

6/15/47

3.7.1.3 Confidential and Restricted: Confidential and Restricted material may be transmitted between offices by such means as the chief of the sending office may consider adequate to the protection of its security.

3.7.2 Transmission within the United States:

3.7.2.1 Top Secret: Top Secret material will be transmitted by officer courier or authorized civilian courier. The names of persons who are authorized couriers for Top Secret material may be obtained from the Security Office. The transmission of Top Secret material shall be under the supervision of the Security Office. Under no circumstances will Top Secret material be transmitted by U. S. registered mail. Top Secret couriers will be furnished locked room accommodations when traveling by train.

3.7.2.2 Secret: Secret material shall be transmitted by officer courier, authorized civilian courier, or U. S. registered mail, return registry receipt requested. Secret material may be transmitted between government agencies by messengers of the JRDB with the approval of the Security Officer.

3.7.2.3 Confidential: Confidential material shall be transmitted in the same manner as Secret, except that return registry receipts are not required. Confidential documents will be cleared for transmission by the mail control desk.

3.7.2.4 Restricted: Restricted material may be transmitted by any means providing a reasonable degree of security.

3.7.3 Transmission outside the United States: Classified documents to be mailed to addresses outside the continental limits of the United States must be cleared through the Security Officer.

3.7.4 Telephone Transmission: Classified information of a classification higher than Restricted may not be transmitted by telephone. References to material of higher classification may be made by number, date, etc., provided care is exercised in not revealing substantial classified information.

3.8 The Duplication of Classified Material.

3.8.1 Authorization: Top Secret, Secret, and Confidential material may not be reproduced, except upon authorization of

the Executive Secretary, his deputy, or other authorized person.* Classified material shall be reproduced with a minimum number of copies, because the risk that classified material may fall into unauthorized hands increases in proportion to the number of copies in existence. Whenever the complete text of an original document is copied, all copies of the document must be marked "TRUE COPY"; if only a portion of an original document is copied, all such copies must be marked "COPY."

3.8.2 Securing Log Numbers: Before any Top Secret or Secret document is reproduced, a log number must be assigned. Log numbers for Top Secret documents are assigned by the Security Office; log numbers for Secret documents are assigned by the mail control desk. Log numbers shall be placed in the upper right-hand corner of the stencils or master sheets in such a way that all copies will carry the log number.

3.8.3 Marking or Stamping Classified Documents, Drawings, and Tracings: The classification shall be typed on the top and bottom of the stencils or placed on the reproduction sheets in such a way that all copies will carry the classification at the top and bottom of the pages. Classified

* See Oath of Secrecy, Par. 2, (Chapter 3, Section 3.1.2).

drawings or tracings shall carry a legend as to the proper classification in such a way that it will be reproduced in all copies. Whenever practicable, classified photographic negatives shall be marked in the same way.

The top marking must be so placed that it will not be obscured by paper clips, staples, or file fasteners.
If more than 25 copies of a document of more than one page (and if the classification is below Top Secret) are to be prepared, the classification may be typed on the stencils, top and bottom of each page. However, the first page of the document must also be stamped at top and bottom of the page. If fewer than 25 copies are prepared, the classification will be stamped in addition to being typed, on all pages at top and bottom.

All classified documents must bear (either typed or stamped) the following reference to the Espionage Act:

> This document contains information affecting the national defense of the United States within the meaning of the Espionage Act (U.S.C. 50:31 32). The transmission of this document or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

3.8.4 Prohibitions with Respect to Cryptographic Communications: True copies will not be made of any communication transmitted by cryptographic means.

3.8.5 Special Provisions for the Reproduction of Top Secret Material: Top Secret material may be reproduced only under the supervision of a commissioned officer or personnel at the policy-making level. The office initiating the reproduction of Top Secret material shall furnish the person to supervise the reproduction. The mimeograph machine shall be operated only by the authorized Top Secret personnel listed in Appendix II to this Chapter. The Security Office shall be responsible for teaching personnel listed in the Appendix to operate the mimeograph machine.

The maximum number of copies of Top Secret material which may be reproduced is 25, unless authorization for additional copies is given by the Security Office or the Administrative Secretary.*

Persons supervising the reproduction of Top Secret material shall have the following responsibilities:

* The maximum number of copies of SECRET material which may be reproduced is 60, unless authorization for additional copies is given by the Security Office or the Administrative Secretary.

(1) That unauthorized persons do not handle or read Top Secret documents while they are being reproduced;

(2) That the stencils and the backing sheets for stencils are removed from the machine and turned over to the Security Office for destruction;

(3) That spoiled sheets and any waste paper which result from the operation are turned over to the Security Office for destruction.

3.8.6 Destruction of Waste Material: All carbon paper, rough drafts, stenographic notes, spoiled sheets, and any other waste material which accumulates in the reproduction of classified documents must be destroyed in accordance with Section 3.6.7 of this chapter. The only exception is waste material resulting from the reproduction of Top Secret material, which must be turned over to the Security Office for destruction (see Section 3.8.5).

3.8.7 Stowage of Stencils: Stencils may not be saved for re-runs unless they are stored in the same security as that of the documents run off from them.

3.8.8 Distribution of Classified Documents: When Top Secret or Secret documents are prepared for more than one addressee, the office responsible for the preparation of the correspondence or documents will prepare a Distribution Sheet

which will accompany the correspondence or documents--to the Security Office in the case of Top Secret, or to the mail control desk in the case of Secret. Secret and Top Secret material will not be distributed unless the distribution sheet accompanies the documents.

3.8.9 Limitations as to Facilities Which May Be Used for the Reproduction of Classified Information: Classified documents may be reproduced only through facilities maintained by the Secretariat of the Board, unless express permission is given by the Security Office for the use of other facilities which have been approved by the Services for the reproduction of classified matter.

3.9 The Grading (Assignment of Classification) of Documents.

3.9.1 Authority to Classify: Documents may be classified Top Secret or lower by any of the following persons:

(1) Any member of the Policy Council

(2) Scientific Advisors to the Policy Council

(3) Any member of the Executive Council

(4) The Chairman or Executive Director of any JRDB Committee or Panel

Documents may be classified Secret, Confidential or Restricted by the following persons:

(1) All military personnel

(2) Any member of the Policy Council

(3) Scientific Advisors to the Policy Council

(4) Any member of the Executive Council

(5) The Chairman or Executive Director of any JRDB Committee or Panel

Each document shall be classified according to its own content and not according to its relationship with any other document. A letter of transmittal shall bear the highest classification of any of its enclosures, but it may also bear the following notation: "Unclassified upon Removal of Enclosures."

3.9.2 Downgrading: Documents may be declassified only by the office of origin. When practicable in the preparation of a document by an office of JRDB, the approximate date that the document will cease to remain in its present classification will be shown at the top of the document in the following manner:

THE JOINT RESEARCH AND DEVELOPMENT BOARD
Washington 25, D. C.

Effective until _____, at which time the classification is changed to _____.

The use of the form is not restricted to any particular classification.

For declassifying classified documents originating in JRDB, the following procedure will govern:

(1) All persons authorized to classify material under Section 3.9.1 of these regulations may downgrade documents prepared by their committee or panel;

(2) When it is determined that material will be downgraded, the office desiring to reduce the classification will prepare a letter to go to all original addressees, notifying them of the change in classification.

(a) In all cases, copies of letters changing classification shall be sent to the Security Office.

3.10 The Periodic Review of Classified Documents.

Periodic surveys should be made of all files in order to (1) downgrade papers where appropriate; (2) eliminate unnecessary papers. Persons in charge of such surveys should notify the Security Office of all papers which they feel could be destroyed, giving the following information:

(1) office of origin

(2) date

(3) file number

(4) subject

(5) classification

6/15/47

Personnel of the Board are warned, however, that official Government records* may not be destroyed except in accordance with specific federal statute.

3.11 Publicity Clearance.

Information concerning the Joint Research and Development Board shall be released only upon authorization of the Executive Secretary or his delegated deputy in accordance with Chapter 8 of this Manual.

3.12 Authority and Functions of PBA Guards.

The Public Buildings Administration guards are employees of the Federal Works Agency and are on duty in all Government buildings and offices which desire their services. The duties of the guards as they affect members of JRDB are as follows:

(1) Inspection of brief cases and parcels. PBA guards are authorized and required to make periodical spot checks of brief cases and parcels being taken from the building;

* "Records" are defined as "all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received in pursuance of Federal Law or in connection with the transaction of public business, and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data contained therein." (See Act of 6 July 1945, Public Law 133, 79th Congress.) The term "records" will not be construed to include extra copies, or copies made purely for information purposes.

(2) The PBA guards are required by their rules and regulations to have people who desire to enter the building after the close of the business day or on Saturdays, Sundays, and legal holidays, sign a register in the lobby when they enter and sign again upon departure. A person must show proper identification to the guard to gain admittance to to the building.

3.13 Limited Distribution.

A special supplement (Supplement 1) providing instructions on this subject may be obtained by qualified personnel upon application to the Administrative Secretary.

3.14 Exchange of Information.

A special supplement (Supplement 2) providing instructions on this subject may be obtained by qualified personnel upon application to the Administrative Secretary.

6/15/47

APPENDIX I

List of Personnel
Authorized to Sign Property Passes

This appendix will be issued at a later date.

6/15/47

APPENDIX II

List of Personnel
Authorized to Handle Top Secret Material

This appendix will be issued at a later date.

6/15/47

THE NATIONAL MILITARY ESTABLISHMENT
RESEARCH AND DEVELOPMENT BOARD

SECURITY REGULATIONS

REVISED 15 JUNE 1948

ADMINISTRATIVE SERIES NO. 5

RDB 74/2