Mark; REF ID:A70871

This is an excellent study

Suggest putting it in suspense until say Nov 1 — when maybe will know what's what.

F.

File Control Survey

W. D., A. G. O. Form No. 0105
March 27, 1946

24-20956

Declassified and approved for release by NSA on 06-04-2014 pursuant to E.O. 13526

WFF:
Here is our file copy of Control Survey of General Cryptanalytic Problem. The recommendations have been approved by Col. Hayes (i.e. he concurred in the whole paper). It comes out with our views on how it should be organized and should be a useful aid in present reorganization.

MR

REF ID:A70871

SPSIS-1A

31 August 1945

MEMORANDUM FOR COMMANDING GENERAL, SIGNAL SECURITY AGENCY

SUBJECT: General Cryptanalytic Problem

DISCUSSION

1. A Control Office survey of the operations of the General Cryptanalytic Branch was undertaken during the month of July. It became evident from the first that it was not possible to limit this survey to the General Cryptanalytic Branch alone, but that it would be essential to extend the study to include operations integrally associated with the problem which were under other separate administration. The survey therefore reviewed the General Cryptanalytic Problem as a whole.

2. The General Cryptanalytic Problem is considered to be the production of intelligence from foreign communications other than those of the Japanese Army. This approach necessitated a survey of the General Cryptanalytic Branch, the General Analysis Section and the Records and Distribution Subsection of Traffic Analysis and Control Branch, the Information Section of Information and Liaison Branch, and the Diplomatic, Military Attache, and Commercial Translation Sections of the Language Branch.

3. The consideration which was uppermost in the minds of the survey group was the fact that the General Cryptanalytic Problem will be the major function of the post-war signal intelligence activity. With this in view, the functions and the integration of the parts of the problem were considered in the light of their ability to function effectively immediately after the cessation of hostilities with the most efficient use of personnel, space and equipment.

4. The survey was conducted in the same manner as the survey of the Japanese Army Problem previously. The Assistant Director of Communications Research was associated with the Control Office during the course of the study, and a representative of the Chief of the Intelligence Division was present at all of the meetings. Each unit surveyed prepared a check list, which is attached as Tab A. The preparation of the check list not only insured that each survey followed the same general pattern, but also, its preparation necessitated a careful analysis by the section chief of the operations of his section, with the result that he, himself, discovered many improvements in operations which he could effect immediately or bring up at the general meeting for discussion. Following the preparation of the check list, meetings were held with each unit.

SPSIS-1A (31 August 1945)

5. Problems of a more or less routine operational nature, such as specific cases of inadequacy of illumination, dissatisfaction because of grades and promotions, etc., were handled, as far as possible as the survey progressed, by reference to the proper authority.

6. A description of the typical work flow in the General Cryptanalytic Problem has been prepared and is attached as Tab B. The reports on each of the individual sections are attached as Tabs C through O. These reports are limited in general to a description of the organization and functions of each section.

7. The examination of the overall operations of the General Cryptanalytic Problem revealed many difficulties which were common to most of the sections. These problems can be considered as arising from four fundamental difficulties:

a. Administrative separation of integral parts of the problem.

b. Physical separation of units whose work should be closely integrated.

c. Difficulties of personnel procurement and administration.

d. Lack of existence of a method of applying priorities based on consideration of all the elements involved or systematic review of the results obtained.

8. <u>Administrative Separation of Integral Parts of the Problem.</u>

a. The administrative and organizational philosophy under which the operations of the Agency have been conducted over the past year or two has resulted in separating functions which are fundamental to the performance of a mission from the office to which the responsibility for that mission is primarily assigned.

b. A typical example of this has been the placing of the IBM equipment and personnel under an administration which is separate from, and therefore out of the control of, the operations which it serves. This was apparently done out of consideration principally for the size of the IBM group and without consideration of the fact that a piece of IBM equipment is a tool, as are pencil and paper, for the technician who is performing one of the basic operations of signal intelligence activities. The result of this has been that the cryptanalysts who should be as familiar with IBM machines as they are with pencil and paper, mathematics of probability and statistics, Remington Subtractor machines, etc., have been so separated from these machines as to become familiar only with the general processes of use of IBM equipment. It is the opinion of a large number of cryptanalysts that this fact has constantly proved a hindrance to the progress of the work.

c. This philosophy has pervaded even further into the operations, so that it can be seen at work within the Intelligence Division. Here a recognition of the existence of two basic operations whose work could be and in essence was easily separated, i.e., the Japanese Army Problem and the General Cryptanalytic Problem, was subordinated to a concept of branches, attempting to combine all activities which were similar in essence but different in scope and matter. For example, the Information Section of the Information and Liaison Branch, which collects and supplies information almost exclusively for the General Cryptanalytic Problem (the Shipping and Order of Battle Sections serving the same purpose for the Japanese Army Problem) has always been administered separately from the operations with which its work was most intimately connected. The separation of a group such as the Information Section from the operation which it serves gives rise to unnecessary problems of coordination. It means that problems of coordination of several facets of one basic activity have had to be coordinated through the Chief of the Intelligence Division, instead of being completely coordinated, as they could have been by an officer charged with the responsibility for the General Cryptanalytic Problem as a whole. (This same fact is true of the parts of the Japanese Army Problem and was recognized in the expression of a need for a Coordinator of the Japanese Army Problem, which was set forth in the control survey of that problem.)

d. This same philosophy was evident in the manner in which the Japanese Language has been administered. In this case also, the number of persons involved in the process and the problems of their administration was given preference over the requirements of technical efficiency which militate in favor of their integration into the cryptanalytic problems which the linguistic personnel served. This has also meant that any of the problems of the sections of the General Cryptanalytic Branch engaged in the solution of the Japanese systems other than those of the Army have had to be coordinated by the Chief of the Intelligence Division instead of at the source of the problem.

e. Similarly, the organization of the Traffic Analysis and Control Branch has resulted in the separation of certain basic functions from the operations with which they should have been integrated in the first instance. The analysis of the traffic of the Special German Diplomatic Net, the Japanese Domestic Net, the Far Eastern Diplomatic Net, and even to some extent the International Point to Point Networks, is an operation which bears directly on the solution and translation of messages. The interrelation of these activities has been recognized more clearly by the gravitation of the different operations to each other in the form of informal personal contact than by the organization structure which has separated them administratively.

9. <u>Physical Separation of Units Whose Work Should be Closely Integrated.</u>

a. Added to the difficulties of administrative control, geographic location of parts of the General Cryptanalytic Problem has been so arranged as to place serious handicaps in the way of most effective operation. Within itself, the General Cryptanalytic Branch has been divided almost equally between the two operations buildings. This has made difficult close contact between the Branch Chief and the sections of his branch. Likewise, it has given rise to numerous difficulties attendant on the passing of correspondence and directives of any degree of urgency between the two buildings.

b. The separation of two of the most productive of the diplomatic sections from both the Information Section and the Bulletin Section has been costly in terms of time and accuracy. Having been made aware on all sides of a lack of coordination between the Information Section and the operating sections of the General Cryptanalytic Branch, a meeting was held during the course of the control survey between the responsible persons in the Information Section and the principal bookbreakers and translators of the General Cryptanalytic Branch. Two facts were found to be outstanding during the course of an open discussion of ways of more closely integrating the activities of these two groups of people.

c. The first of these was that the administrative separation under which they worked had not been effective in orienting the two groups toward a common goal, and second, that the physical separation of the groups had actually prevented proper use being made of the facilities offered by the Information Section. The most striking proof of the latter fact was given by the head of the Topical Index Subsection of the Information Section, who said that since the Romance Language and the Miscellaneous Language Sections of the General Cryptanalytic Branch had moved to Operations "A" Building, the number of questions asked of his section had dropped by nearly half. Fully aware that the number of questions needing to be answered had not dropped, the conclusion that there was so much time and labor involved in transacting business by telephone or by walking the distance between the two buildings that questions simply were not asked was substantiated by the translators and bookbreakers of the General Cryptanalytic Branch.

d. Although by now the disappearance of the Japanese Military Attache some Japanese Diplomatic traffic has decreased the importance of the problem, the separation of the Japanese Diplomatic Translation Section of the Language Branch from the Japanese Diplomatic Section of the General Cryptanalytic Branch presented just such a case of waste motion and time caused by physical separation. The units performing all of the cryptanalytic and cryptographic processes on Japanese Diplomatic messages were located in the fourth wing of the first floor; the translators were located in the headhouse opposite the first wing on the second floor. Every Japanese Diplomatic message had to be carried twice between these two offices. The amount of time spent in carrying these messages back and forth has been enormous.

SPSIS-1A (31 August 1945)

10. Difficulties of Personnel Procurement and Administration.

a. From almost all of the operating sections of the General Cryptanalytic Branch and from the Information Section of Information and Liaison Branch, there were expressions of lack of personnel both in quality and quantity. The number of trained cryptanalysts on the post is dangerously few in comparison with the magnitude of the problems presented for solution. Further, linguistic personnel are needed for the production of intelligence in languages for which there are no translators in the Agency. Principal among these are the languages of Central and Southeastern Europe, the Middle East, and the Far East - Czechoslovakian, Serbo-Croatian, Bulgarian, Polish, Greek, Turkish, Arabic, Persian, Chinese. These shortages must be filled if the Signal Security Agency is to accomplish the intelligence aspect of its mission. There is attached as Tab P a staff study on the subject of cryptanalytic personnel which presents some of the problems.

b. There is a generally expressed opinion among the operating personnel that the War Department higher authority is not fully conscious of the uniqueness and importance of the work of this Agency. Their opinion seems to be based on the fact that the salaries and other less material inducements offered by this Agency to men of real ability cannot compare to the salaries offered to such men elsewhere. They recognize that the government employees in general are low paid, but they believe that the contribution of this Agency to the prosecution of the war has been proof enough of the outstanding value of this organization, and they failed to see why steps cannot be taken to attract and keep men of outstanding ability in this work as a career. There is real merit in this opinion.

c. The mechanics of promotion of persons within the Agency afford the basis of another of the most common complaints. The necessity for close adherence by Personnel Branch administration to the Civil Service Regulations in such matters as qualifications, job descriptions, etc., has, in many cases, either prevented the Agency from getting the full benefit of the capabilities of a person on a job he was eminently capable of performing because Civil Service qualification standards prevented his assignment to that job; or has forced the heads of sections to resort to subterfuge, which they themselves have felt as unbefitting. In all too many cases, the choice offered to the head of a section has been to neglect the job to satisfy the regulations or to perform the job by resorting to subterfuge. This well recognized fact, particularly by the higher grades of personnel in the operations, is also laid by them to the lack of recognition of the uniqueness and importance of the work.

d. Further, the technical personnel believe, in many cases, that grades are applied to jobs by persons who have no technical knowledge or very little knowledge of the duties the person is performing.

REF ID:A70871

REF ID:A70871

11. Lack of Adequate Direction from the Intelligence Point of View, and Lack of a Complete Method of Critical Review of the Work Accomplished.

a. For nearly two years the Signal Security Agency acted on the basis of one single, generally worded, intelligence directive. The objective of this directive, which quickly became obsolete, was to direct intercept, determine assignment of personnel to solution and production problems in the order of their importance, and in general, to operate as a priority directive for Signal Security Agency.

b. The inadequacy of such a directive was felt particularly keenly by the General Cryptanalytic Problem because of the variety of the requirements placed upon it in all fields - intercept, solution, translation, etc.

c. Despite the assumption that Signal Security Agency, of itself, was incapable of determining the priority of its work, it was always necessary in fact for the responsible officers here to make decisions as to the relative importance of jobs from an intelligence point of view. However, since such decisions were not officially recognized, no well defined method for arriving at decisions on priorities was ever worked out at the Signal Security Agency.

d. The appointment of a group of officers from the Military Intelligence Service in recent months, whose duty it is to give priority direction to the work of the General Cryptanalytic Branch, has gone far to remedy this situation, but has not solved it. The reasons why it has not solved and cannot solve the problem are two-fold:

(1) First, because the principal user of the product of the General Cryptanalytic Branch is actually the State Department, and the Military Intelligence Service is in only a slightly better position to know the requirements of the State Department than is the Signal Security Agency.

(2) Second, because in the problem of application of priorities intelligence is only one of the bases - the problems of intercept, solution, and translation exert equal influence on the priorities.

e. In addition to the problem of priorities, a system of review of the work of the General Cryptanalytic Problem has never been completely developed, largely because of the pressure of time present throughout the war. Hand in hand with a system of priorities should be a system of review of the work so that an accurate estimate of the effects of the priorities can be made.

REF ID:A7087

f. All of the elements of the mechanism for the setting and reviewing of priorities are present at the Signal Security Agency and the Military Intelligence Service, but they have not been coordinated, and, in fact, their use to this end has generally not been recognized. Attached as Tab 7 is an outline of the requirements for a well developed system for establishing and reviewing priorities.

12. General Difficulties.

a. Illumination. In almost every section the officers in charge pointed to the fact that the illumination of the buildings is inadequate. They estimate that an increase of 25% in the efficiency of the individual workers would be possible if the wings and headhouses were adequately illuminated. Indirect overhead lighting such as is installed at the Naval Communications Annex was highly recommended.

b. Ventilation. Similarly, the heads of sections felt that the efficiency of individual workers suffers greatly from inadequate ventilation both in summer and winter.

c. Research Group. The Research Group of the General Cryptanalytic Branch is composed of the best cryptanalytic brains available. These experts should be available to apply the experience gained from the solution of foreign systems to the security of our own systems. This experience is only available now by means of a very informal arrangement which is not entirely satisfactory.

d. Recorder's Group. The Recorder's Group of the General Cryptanalytic Branch has a mission to perform which can be very important in both the immediate and distant future. If technical descriptions of the methods of solution of all cryptographic systems, all cryptanalytic techniques developed in the last few years, and other technical information were prepared and elaborately cross-indexed, this information would be of utmost value to the Agency. The personnel currently assigned to the Recorder's Group is not adequate to perform the mission.

RECOMMENDATION

1. That any reorganization of the Intelligence Division to meet the post-war requirements take into account and avoid the difficulties pointed out in paragraph 8 of the foregoing.

2. That the reallocation of space be approached in a realistic manner with the purpose of placing all units in the most efficient physical relation to one another.

3. That immediate steps be taken at all costs to take the action recommended in Tab P.

REF ID: A70871

4. That the Assistant Chief of Staff, G-2, be informed of the critical need of this Agency for linguists, mathematicians and engineers; that a list of qualifications be submitted, and the Assistant Chief of Staff, G-2, request of the Adjutant General to inform this Agency of all men discharged from the Army who satisfy these qualifications. (This has been directly recommended to the Personnel Branch.)

5. That promotions of technical personnel be reviewed by a small board of technicians who are capable of judging their ability. Such a board should include men such as Mr. Friedman, Colonel Kullback, and Lt. Colonel Rowlett.

6. That a priorities control and review unit be established, as set forth in Tab Q.

7. That as soon as all plans have been completed for the physical relocation of all of the offices of the Post, the entire lighting system be studied by competent illumination engineers.

8. That when plans for physical relocation have been completed, the necessity for an air-conditioning system be investigated.

9. That the Research Group of the General Cryptanalytic Branch be established with a more formal relationship to security problems. Should the establishment of a Research and Development Division be approved, this group should be incorporated in it.

10. That the Recorder's Group of General Cryptanalytic Branch be augmented in quantity and quality of personnel in order to finish as soon as possible a complete writing up and cross-indexing of technical processes, cryptographic systems, etc.

CONCURRENCES

17 Incls
Tab A - Check List
Tab B - Work Flow w/incl
Tab C - Survey B-4D w/2 incls
Tab D - Survey B-3 Adm w/2 incls
Tab E - Survey B-3A w/2 incls
Tab F - Survey B-3B w/2 incls
Tab G - Survey B-3C w/2 incls
Tab H - Survey B-3D w/2 incls
Tab I - Survey B-3E w/2 incls
Tab J - Survey B-1M
Tab K - Survey B-3F w/2 incls
Tab L - Survey B-1C
Tab M - Survey B-1D w/2 incls
Tab N - Survey B-3G w/incl
Tab O - Survey IR-6 w/2 incls
Tab P - Study - Procurement of Personnel
Tab Q - Proposed Priorities Control Unit

JAMES H. FRIEP, JR.
Major, Signal Corps
Control Officer

CONTROL OFFICE SURVEY

1. A continuing survey of operational and administrative procedures is being conducted by the Control Office in order to:

a. Discover any possible improvements which may be effected in operational efficiency.

b. Evaluate the use of personnel and space.

c. Examine relation of unit surveyed to other units.

2. No claim is made by those conducting the survey as to technical knowledge which would permit them to originate suggestions of value as to the techniques employed. However, by a review of operations, those experienced in each are themselves led to suggest possible improvements, and hence, it is from this personnel that the most worthwhile suggestions are expected.

3. Sometimes operations are in effect where output does not justify the expense involved, but are continued only because of habit. Files are continued which are unnecessary.

4. Also, operatives have ideas as to possible improvements which they have not effected because of lack of time to interrupt their daily work. A survey such as this affords the opportunity to discuss all phases of the operation of each unit; to examine all ideas and suggestions as to possible measures to improve procedure; to eliminate unnecessary work; reduce reports; in a word, to review all activities of each unit.

5. It is desired to interrupt operations as little as possible, and the attached check list is a step towards this end. The check list should be completed and returned to the Control Office with the requested material attached.

TAB
A

CONTROL OFFICE SURVEY

1. A continuing survey of operational and administrative procedures is being conducted by the Control Office in order to:

a. Discover any possible improvements which may be effected in operational efficiency.

b. Evaluate the use of personnel and space.

c. Examine relation of unit surveyed to other units.

2. No claim is made by those conducting the survey as to technical knowledge which would permit them to originate suggestions of value as to the techniques employed. However, by a review of operations, those experienced in each are themselves led to suggest possible improvements, and hence, it is from this personnel that the most worthwhile suggestions are expected.

3. Sometimes operations are in effect where output does not justify the expense involved, but are continued only because of habit. Files are continued which are unnecessary.

4. Also, operatives have ideas as to possible improvements which they have not effected because of lack of time to interrupt their daily work. A survey such as this affords the opportunity to discuss all phases of the operation of each unit; to examine all ideas and suggestions as to possible measures to improve procedure; to eliminate unnecessary work; reduce reports; in a word, to review all activities of each unit.

5. It is desired to interrupt operations as little as possible, and the attached check list is a step towards this end. The check list should be completed and returned to the Control Office with the requested material attached.

MATERIAL REQUIRED AS PRELIMINARY TO SURVEY

1. Space allocation - to be prepared by Control Office.

2. Work flow chart - on 1 above, draw in the flow of work.

3. Organization chart of unit. (If one is not available, furnish a rough diagram to Control Office.)

4. Data on assigned personnel:

   a. Number of officers — Male _____ WAC _____

   b. Number of enlisted personnel — Male _____ WAC _____

   c. Number of civilians

   d. Total

CHECK LIST FOR INVESTIGATIONS

1. The following questions are to be answered as briefly as possible:

   a. Mission - Statement of mission (general) by subsection.

   b. Operations:

      (1) What units work in close liaison with your section?

(2) Is personnel assigned adequate for mission? If not, state requirements by subsection.

(3) Have requirements been requisitioned?

(4) Difficulties arising pertaining to personnel.

(a) Promotion

(b) Dissatisfaction

(c) Others

d. Space:

(a) Is space adequate? If not, state requirements.

(b) Is location convenient for contact with other sections with whom you work?

e. Lighting:

Is lighting adequate?

f. Files:

(1) What files are maintained? (be specific)

(2) How long is material kept?

(3) Suggestions for eliminating unnecessary files or disposing of obsolete files.

(4) What functions and records have been discontinued in last six months?

g. Correspondence - What type is carried on?

h. Reports

(1) What reports are rendered by each unit, and what distribution is made?

(2) Suggestions for eliminating unnecessary reports.

(3) What is used as reference material, how handled, how long kept?

i. General - Suggestions as to steps possible for improvement in operation of your unit?

REF ID: A70871

TAB
B

WORK FLOW IN THE GENERAL CRYPTANALYTIC PROBLEM

1. To present the interrelation of all of the parts of the General Cryptanalytic Problem in the clearest manner possible, this description of the flow of work in the present organization in this problem has been prepared. The method of presentation is to follow the flow of messages through the various sections and units, outlining in some detail the processing to which it is subjected in each of the sections. A chart, illustrating the work flow of traffic in the General Cryptanalytic Problem, is attached herewith.

2. The traffic which pertains to the General Cryptanalytic Problem is intercepted in the largest measure by fixed stations under the direct control of the Signal Security Agency, the Office of the Chief Cable Censor, and United Kingdom Intercept Stations. These sources of the raw material are all in communication with the Signal Security Agency by teletype, but several different practices are employed in the submission of the traffic.

a. The stations under the direct control of the Signal Security Agency submit all government traffic by teletype unless specifically requested to do otherwise; and non-governmental is sent by mail.

b. The Office of the Chief Cable Censor is capable of handling only a limited volume of traffic over the teletype channels between this Agency and that Office. To make the best use of these teletype facilities, a list of the types and nationalities of traffic desired by teletype is drawn up at the Signal Security Agency, and all other traffic, both governmental and non-governmental, is forwarded by mail.

c. Since the cost of the transmission of traffic by wire from the United Kingdom to the United States is high, it is desired to keep the amount of intercept traffic received by wire from the British to the minimum commensurate with complete coverage. To this end a request is periodically submitted to the British, listing the cryptographic systems and the radio circuits from which traffic is desired at the Signal Security Agency by the fastest possible means. All other governmental traffic which the exchange agreements make available to the United States is forwarded to the United States by air bag.

3. All of this incoming traffic, both teletype and mail, is received in the Traffic Section of the Communications Branch of the Operating Services Division.

4. From this section, the traffic is immediately passed to the Records and Distribution Subsection of the Traffic Section of the Traffic Analysis and Control Branch. It is in this subsection that the processing of traffic begins.

5. All teletype traffic and mail traffic from most of the United States stations is received in three copies; mail traffic from other

sources generally in single copy. Since the greatest volume of diplomatic traffic is received by teletype or from United States stations, this type of copy will be considered as forming the basis for the operation and single copies will be considered as exceptions or variations in the rule. The first step performed in the processing of the traffic in the Records and Distribution Subsection is the cutting of the teletype sheets into individual message lengths. All traffic is then sorted by type and nationality and is sent to units of this subsection for further processing. The processing performed in these units is the identification of the cryptographic system in terms of the trigraphic designation which has been assigned to each unique cryptographic system, or the identification of traffic by certain types, such as Navy, Commercial code, etc., to which arbitrary trigraphic designations have likewise been assigned. The criteria which are used in these units for the identification of systems and types of traffic are supplied to them by the national units of the General Cryptanalytic Branch. These criteria usually include unique addresses, system discriminants, common code groups, signatures, etc. The trigraph is written on all three copies of the traffic together with a number which identifies the clerk handling the traffic. A record is kept in this section of the volume of traffic received from each of the sources by type and nationality and by method of submission, i.e., wire or mail. The messages are then ready for forwarding.

6. The first copy of the message is sent to the sections of the General Cryptanalytic Branch. Since the processing of this copy requires the most elaboration, the description of its handling is covered last. The second copies of the messages are forwarded to the General Analysis Section of the Traffic Analysis and Control Branch, and the third copies to the British Exchange Unit of the Traffic Section of the Operating Services Division.

7. Processing in the General Analysis Section.

a. As is easily understood, it is impossible to intercept all of the traffic which appears on the air. The problem at the Signal Security Agency is to employ intelligent selectivity in the interception of as much traffic as our intercept facilities will permit. To this end, it is the function of the General Analysis Section to conduct such studies and maintain such records in connection with the interception of traffic from all radio networks other than Japanese Army, as will enable the most intelligent directives to be given to increase the effectiveness of the intercept coverage of these networks.

b. The sources of information used in the preparation of these studies and reports are the daily logs indicating intercept performance, submitted by each monitor station, and the second copy of the raw traffic.

(1) From the intercept station logs which show the radio stations from which traffic was copied, the receiving stations which they contacted, the period of time during

TOP SECRET

which the station was heard, and the strength and the readability of the signal, graphs are prepared which show the period of activity of each transmitting station, and the effectiveness with which our monitoring station is capable of copying traffic sent by each station.

(2) From the preambles of the messages and from the trigraph written on the message, data are prepared and maintained which list the quantity of traffic passing over all city-to-city and station-to-station circuits by cryptographic system.

(3) From a study of duplicate transmissions over a long period of time, information on the routing procedures employed by the various radio stations in passing traffic over long distances is collected.

c. Current information on changes in call signs, frequencies, station operations, etc., is maintained so that monitor stations can be informed immediately of these changes, and their intercept assignments altered to reflect them. As has been pointed out before, it is not possible to monitor all transmissions which pass over the air. What is attempted, then, is to adjust intercept missions on the basis of information as described above, in such a way as to intercept the greatest amount of traffic desired by the Signal Security Agency, and ultimately by the Military Intelligence Service. This must be done on a priority basis. In order to establish this priority, the representatives of the Military Intelligence Service and the General Cryptanalytic Branch prepare a list of the cryptographic systems and the city-to-city circuits in the order in which they desire the greatest amount of coverage. Their priority listing contains five classes:

(1) "A" Priority. This includes systems and circuits for which complete coverage is desired, regardless of the cost.

(2) "B" Priority. This class includes the most important systems of principal countries. Complete coverage of the systems and circuits contained in this list is desired at the expense of lower priority traffic, and an attempt is made to get this coverage at a minimum of duplication.

(3) "C" Priority. This class is reserved for search missions and temporary assignments. Diplomatic traffic seldom falls in this priority.

(4) "D" Priority. This class includes the run of the mine diplomatic systems. All facilities available after

TOP SECRET

the assignments have been made to secure coverage of higher priority traffic are devoted to this class.

(5) "F" Priority. This class consists of types of messages for which no attempt need be made to obtain coverage. This includes generally plain text, commercial traffic, or obsolete or obsolescence systems.

d. On the basis of the information contained in their records of the volume of traffic passing over station-to-station circuits by cryptographic systems, the General Analysis Section is enabled to convert the statement of priority of cryptographic systems and city-to-city circuits into terms of radio transmitters, stations, and circuits. Circuits which carry "A" priority systems are automatically "A" priority circuits, and all other circuits are listed in order of volume and priority of traffic. The ability of this section to make the conversion of systems to circuits is made possible under this system by the fact that the trigraph appears on the messages which are sent to this section for study. For this reason it is very important that the trigraphing done in the first instance be as accurate as possible.

e. With priorities expressed in terms of radio circuits the General Analysis Section is then in a position to implement priorities. The information obtained in their studies of operating schedules of the transmitting stations, the routing procedures of these stations, and the ability of each monitoring station to cover certain circuits at different hours of the day, permit the assignment of missions to the monitoring stations by call sign and hour of the day in such a manner as to insure the best possible coverage.

8. Processing of Traffic in the British Exchange Unit.

a. The third copies of messages are sent from the Records and Distribution Subsection of the British Exchange Unit. It is the responsibility of this unit to extract, from the mass of traffic, copies of messages which are in systems requested of us by the British, and to forward these copies to the British Security Commission in New York. The messages to be exchanged are identified by the trigraph written on the message. A record is kept in this unit of all messages sent to the British Security Commission.

9. Processing the Messages in the General Cryptanalytic Branch.

a. The first copies of the messages are forwarded from the Records and Distribution Subsection to the appropriate national group within the General Cryptanalytic Branch. The first process to which the messages are subjected in the General Cryptanalytic Branch is indexing.

b. The indexing of intercepted messages has three main purposes - bookkeeping, reference, and providing collateral information for the cryptanalysts.

TOP SECRET

(1) Bookkeeping. The Signal Security Agency is responsible for each message received in the same manner as any business office is responsible for every piece of equipment, invoice, or order that it receives. In a sense, every intercepted message received at the Signal Security Agency is an order of the cryptanalyst and translator to produce the intelligence contained in it. In order to be certain that every order is fulfilled to the best of our ability, a method of accounting for each message and the disposition of it has been established.

(2) Reference. Each of the national groups of the General Cryptanalytic Branch is endeavoring to function in the same manner as the message centers of the countries on whose traffic it works. For this reason, records of the correspondence of the countries are set up in a manner similar to that in which those countries record their own telegraphic correspondence.

(3) Providing Collateral Information for the Cryptanalysts. A great deal of information which is helpful for the solution of cryptographic systems can be gained from a knowledge of the mistakes made by code clerks and message center clerks, such as the enciphering of the same text in two keys, the correction of cryptographic errors in service messages, etc.

c. The index books are set up in such a way as to enable the occurrence of these errors to be called quickly to the attention of the cryptanalysts.

d. Methods of Indexing.

(1) Methods of indexing have been developed in the General Cryptanalytic Branch over the last several years which provide for the accomplishment of all three of these purposes of indexing.

(2) One of the first breakdowns in the indexing books is indicated by the nature of the diplomatic correspondence. In any stable government the diplomatic set-up consists of a central office (the foreign office, state department, or whatever it may be called) and a group of officers located in foreign countries which are responsible to this central organization. The result of this set-up is that the bulk of diplomatic correspondence passes from a central office to its representatives, or vice versa, although there may be some correspondence between outlying offices. Since the messages passing

from each city to each other city almost invariably constitute different sets of correspondence, the index books are generally set up on a city-to-city basis. The order of the messages on the index page is dictated by the order in which the corresponding office arranges them. The most usual order is by the message number assigned to the message by the writer.

(3) The other information which is recorded is the file date of the message, the group count, the trigraph, the intercept source, the intercept date and time, the worksheet number which is used for file purposes, several significant groups of the message, and, later in the processing, the bulletin number.

e. The information contained in the index books is used to accomplish many purposes:

(1) The determination of duplicate texts prevents the duplication of decoding and translating.

(2) Oftentimes the first information concerning a change of a diplomat will be found in the signature of diplomatic correspondence. Especially if a signature is found on a system which is not readable, it is the duty of the indexing personnel to call attention to this change of signature.

(3) Estimates of the percentage of coverage of a circuit can best be made on the basis of the writer's message numbers. If a great many message numbers are being missed, it is the duty of the indexing personnel to call attention to this fact, so that steps will be taken to increase coverage if it is desired.

(4) In addition, a study of message numbers, combined with the information kept in the General Analysis Section, can be used to build up a comprehensive picture of the communications practices of each country.

f. After having been properly indexed, messages are then passed on to other units within the national group for further processing.

g. From the point of view of the activities of the Signal Security Agency, messages fall into four general categories:

(1) Unreadable and not being studied.

(2) Unreadable and being studied.

(3) Readable but requiring considerable cryptanalytic effort.

(4) Completely readable.

h. Messages may fall into category (1) because of lack of traffic, lack of personnel, or low priority in the working order. Messages in such systems are filed either within the indexing unit or in the research unit of the national group.

i. Messages which are in systems unreadable but being studied are passed from the indexing unit to the research unit of the national group to be added to the traffic under study. These unreadable systems are studied by the research unit to discover first the nature of the system. When this has been determined, existing cryptanalytic techniques, by use of which other similar systems have been solved, are applied. In addition, new techniques which may be applicable to the system at hand are devised. Very often it is necessary and desirable to call upon the assistance of the Research Group of the General Cryptanalytic Branch, which is composed of the most experienced and competent cryptanalysts available. The members of this research staff come and study the problem and recommend methods of approach to solution. When the solution has been accomplished, that is, when the proper technique for solving the elements has been determined and tests have shown their effectiveness, the system is usually turned over to an exploitation group for the solution of all of the elements of the system through the employment of cryptanalytic techniques.

j. Messages in systems which are readable but require the expenditure of cryptanalytic effort are passed to the cryptanalytic exploitation unit within the national group. An exploitation group is usually composed of good cryptanalysts and cryptanalytic aides who often use very complicated and difficult cryptanalytic techniques to solve all of the elements of a system and reduce it to a stage where messages can be immediately deciphered and decoded. These groups are usually concerned with cipher systems and systems of encipherment, code solution being essentially the application of linguistic techniques. These exploitation groups usually work hand in hand with the bookbreakers who are reducing to code book to a stage where messages can be decoded immediately on receipt.

k. Messages which are in systems which are already readable are passed to the decoding and deciphering unit of this group. The decoding and deciphering unit applies the enciphering key which has been recovered by the exploitation unit and decodes the messages from code books which have been recovered by the bookbreakers.

l. Constant recourse is had by the national groups to the Information Section of Information and Liaison Branch, principally in the processing of messages during bookbreaking and translating. Collateral information is of great use in the process of bookbreaking and additive recovery. For the purpose of making the greatest amount of collateral information available to the cryptanalysts and translators, the Information Section of Information and Liaison Branch has set up files and conducted studies along the following lines:

(1) Biographical files which contain names of individuals taken from ultra sources, the newspapers, and other documents of all sorts.

(2) Geographical files and atlases.

(3) A topical index file in which all subjects appearing in the diplomatic bulletin series are cross indexed by subject matter, to be made available at a future time to the cryptanalysts and bookbreakers; the scanning and dissemination of all incoming documents to attempt to get such information as will be of value to cryptanalysts and translators to their immediate attention.

m. The Information Section also conducts special studies of events of political and economical import, personalities, and of areas of the world, on request from the national groups. The information so collected is made available principally through the use of the secure telephone system, by means of which the person desiring information calls the Information Section and states specific questions. The files and records of the Information Section are examined to find the answer to the question, and if it is not found here, it is normally referred to the Military Intelligence Service or Naval Intelligence to see if these agencies are able to supply the answer. The originator of the question is then called on the secure phone and the answer given.

n. Messages which have been decoded and deciphered are turned over to the translating units where they are scanned to determine if the information contained in the messages is of sufficient intelligence value to warrant publishing. This scanning is accomplished on the basis of information made available from the Military Intelligence Service as to their desires, and from the knowledge of the translating personnel of the current political and economic situation. Messages which are considered of great importance are translated in full. Those which contain some information of value are summarized, with emphasis on information which may be in the message which is of value. Messages which do not seem to contain information of importance are filed without being translated or summarized. The finished translations or summaries are then sent to the Bulletin Section of Information and Liaison Branch. This section assigns a publication number in one of the series reserved for diplomatic traffic, types ditto stencils of the messages, runs off ditto copies and disseminates these copies according to a dissemination list prepared by Military Intelligence Service and Signal Security Agency.

o. A copy of the published message is returned to the national group where the published number is entered in the index book for future reference, and the bulletin copy is filed.

10. This is a general picture of the handling of diplomatic messages. In any particular section the practices may vary to a slight extent, but this presentation of the flow of messages through the sections handling diplomatic traffic may be considered to represent the normal.

1 Incl
Work Flow Chart

REF ID:A70871

GENERAL ANALYSIS SECTION, SPSIB-4D
TRAFFIC ANALYSIS AND CONTROL BRANCH, SPSIB-4

TAB C

1. The mission of the General Analysis Section of the Traffic Analysis and Control Branch is:

a. To maintain records and conduct analytical studies to provide information for the assignment of intercept missions on coverage of commercial radio stations passing diplomatic, military and naval attache, press, commercial and other types of point-to-point radio traffic.

b. To maintain records and conduct analytical studies to provide information for the assignment of intercept missions on coverage of the Japanese Domestic Net, Japanese Far Eastern Diplomatic Net, weather stations, and radiotelephone circuits.

c. To compile and publish for dissemination to intercept stations and/or other offices within the Signal Security Agency, reports on the operations of the Far Eastern Diplomatic Net and the Japanese Domestic Net.

d. To operate a Kana Sorting Unit to insure that intercepted plain text Kana traffic and encoded Kana syllable traffic is properly trigraphed and distributed to other offices within the Intelligence Division and/or other agencies, as prescribed by proper authority.

2. In the performance of this mission the General Analysis Section is organized into two subsections and eight units, as illustrated on the organization chart attached as Inclosure 1.

3. The following are the units with which the General Analysis Section maintains close liaison:

a. Records and Distribution Subsection of Traffic Section of Traffic Analysis and Control Branch.

b. Machine Branch.

c. Planning and Priorities Office of General Cryptanalytic Branch.

d. Facilities Section of Communications Branch.

e. British Exchange Unit.

f. Message Center.

g. Second Signal Service Battalion.

4. Personnel.

a. The following is a list of the personnel employed in the General Analysis Section:

Male Officers	- 3
WAC Officers	- 3
Enlisted Men	- 1
Enlisted WAC	- 4
Military Personnel	- 11
Civilians	- 66
Total Personnel	- 77

b. The above personnel is adequate to perform the mission of the section.

c. There are no outstanding personnel difficulties.

5. The General Analysis Section is located in the second wing, first floor, and the rear of the fourth wing, first floor, of Operations "B". A floor plan of the section is attached as Inclosure 2. The space allotted is adequate, but its location in respect to other units of the General Cryptanalytic Problem is not altogether adequate.

6. The lighting is adequate, but improvement in the lighting system would be a definite benefit.

7. Files.

a. The following files are maintained in the General Analysis Section.

(1) Edited Traffic. All edited diplomatic traffic, from every source, is filed - 100 messages to a book - and kept in the files for three months. Mail traffic is logged, and the log sheets are also kept for a three-month period. Traffic on file dates from 1 March 1945.

(2) Daily Coverage Reports. Shows the results of each Monitoring Station's commercial assignments on a daily basis. The circuits assigned, but not copied, are listed with their frequency, priority, and any other monitoring station which picked up the call. Also, any unassigned call signs heard are listed. Reports on file from August 1943 to present date.

(3) Contact Card File. There is a card for each call sign monitored on the commercial assignments of each intercept station devoted to commercial traffic. To these cards are posted daily the calling station, receiving station, and the Monitoring Stations which pick up the call. On file from November 1944 to date.

(4) Original Log Sheets. Original teletype daily logs from United States Monitoring Station and the Canadian Stations. On file from March 1944 to date.

(5) Schedule "A". Schedule "A" shows our complete monitoring assignments, arranged alphabetically according to country monitored. The purpose of the Schedule is to inform the British and Canadian intercept operators of the call signs we monitor. The schedule shows the country, station, call sign, frequency, period of coverage, contacts, and our Signal Security Agency stations which monitor each call. On file from December 1943 to date.

(6) Basic Coverage Sheets. There is a sheet for each call sign, with its frequency and Monitoring Station. The contacts made by this call sign are indicated by the hours heard, and the readability is shown by using blue pencil for good strength, green for fair, and red for poor reception. These sheets are used in making commercial intercept assignments. On file from April 1943 to date.

(7) Daily IBM Run Books. Purpose: To make current reports on coverage of intercept missions. All edited commercial traffic for one day, intercepted from every source, is listed in the Daily Run, first according to sending call sign, then receiving call sign, intercept date and time, and radio circuit number. These runs are destroyed after each Weekly Run is received.

(8) Weekly IBM Run Books. Purpose: To make weekly reports on coverage of intercept missions. All edited daily diplomatic traffic for one complete week is consolidated in a Weekly Run. The "H" Run is used in making a Weekly Call Sign Priority Report - the sort being on sending call sign, trigraph value, and receiving digraph. The Weekly "A" Run is used in making a Weekly Circuit Priority Report - the sort is on sending call sign, receiving call sign, intercept date and time, and radio circuit. The Weekly "A" runs are destroyed after receipt of the Monthly "A" Run. The "H" Runs are on file in the basement of the cafeteria from July to October 1944. From then on, they are kept in the section from November 1944 to date.

(9) Monthly IBM Run Books. Purpose: To make monthly reports on coverage of intercept missions. All edited daily diplomatic traffic for one complete month is consolidated in a Monthly "A" Run. These runs - from July 1943 to

to June 1944 - are in the basement of the cafeteria; from then to present date - on file in section. The Monthly "C" Run has the main sort on the sending station, then city of destination, and next on the receiving station. These runs - from December 1943 to October 1944 - are in the basement of the cafeteria; from then to present date - on file in section. Monthly "D" Run has the major sort on the country of origin, then the country of destination and the sending station. These runs - from December 1943 to September 1944 - are in the basement of the cafeteria; from September to present date - on file in section.

(10) Frequency Card File. This card file shows the priority of each frequency of the Commercial circuits monitored. Each week this file is brought up to date. New cards are added as monitoring assignments change, and new circuits are monitored. The old cards are kept in file for possible active future use. File kept in section, and has been in use since September 1944.

(11) Weekly Circuit Priority Report and Weekly Call Sign Priority. These reports present the relative value of commercial circuits and commercial call signs, respectively, and are used in making intercept assignments. The circuits and call signs are listed in order of their priority. On file in section since they were first started in July 1944 to present date.

(12) "D" Country-to-Country Circuit Book. These books show the relay points of messages (diplomatic) sent from country to country. They also indicate the number of messages sent monthly from one country to another. The books have been filed in the section since December 1943.

(13) "C" Country-to-Country Circuit Book. Show the relay points and direct circuits over which traffic is routed, from one country to another. They also show the number of diplomatic messages sent. These books have been filed in the section since December 1943.

(14) Activity Chart. This report shows the active circuits with the number of diplomatic messages and their priority values. The report is set up on a monthly basis, although the number of messages are posted weekly. The reports are filed in this section - since their beginning in July 1944.

b. The following functions and records have been discontinued during the last six months:

(1) Curtailment of Schedule "A".

(2) Discontinuance of "1" Runs.

(3) Elimination of Special German Diplomatic Net Unit.

(4) Discontinuance of Weather group.

(5) Curtailment of Non-Morse Unit.

8. The following reports are rendered by the General Analysis Section:

a. Schedule "A".

b. Daily Coverage Reports.

c. Call Sign and Circuit Report.

d. Monthly Japanese Domestic Net Report.

e. Monthly Far Eastern Diplomatic Net Report.

9. Traffic and station logs constitute the basic reference material of this section.

10. A general description of the work of this section is contained in the work flow report in Tab B.

TOP SECRET

REF ID:A70871

GENERAL ANALYSIS SECTION, SPSIB-4D

SECRET

Officer in Charge

Executive Officer

Special Types Sub-Section

SPSIB-4D-1

Officer in Charge

Jap Domestic Net Unit

SPSIB-4D-1A
Civilian in Charge

Kana Sorting Unit

SPSIB-4D-1B
Civilian in Charge

Far Eastern Diplomatic Net Unit
SPSIB-4D-1C
Civilian in Charge

Weather - Non Morse Unit

SPSIB-4D-1D
Civilian in Charge

Commercial Sub-Section

SPSIB-4D-2

Officer in Charge

Traffic Processing Unit

SPSIB-4D-2A
Civilian in Charge

Logging Unit

SPSIB-4D-2B
Civilian in Charge

IBM Analysis Unit

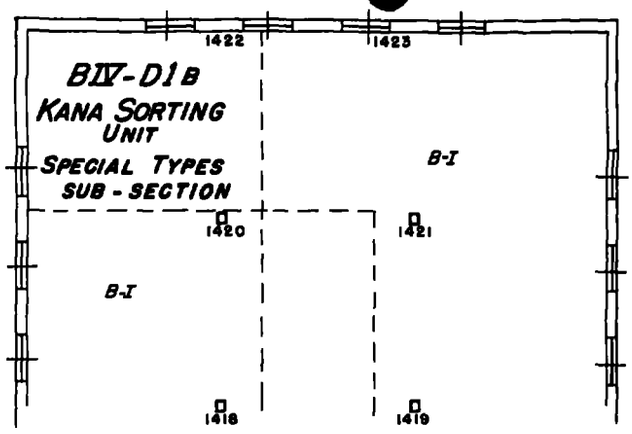
SPSIB-4D-2C
Civilian in Charge

Coverage Analysis Unit

SPSIB-4D-2D
Civilian in Charge

SECRET

REF ID:A70871

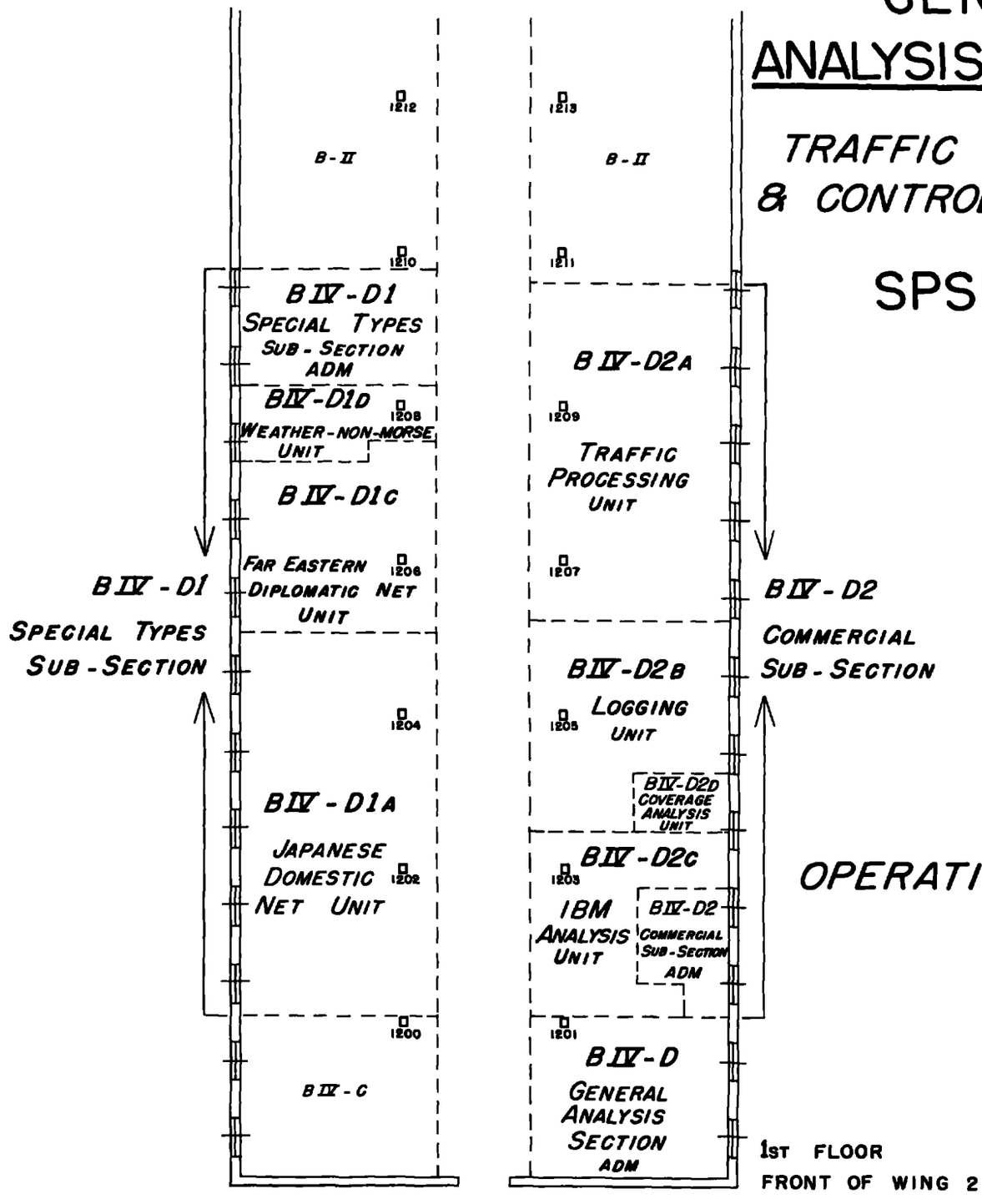


1ST FLOOR
BACK OF WING 4

GENERAL ANALYSIS SECTION

TRAFFIC ANALYSIS & CONTROL BRANCH

SPSIB-IV D



1ST FLOOR
FRONT OF WING 2

OPERATIONS "B"

2

SPSIS-IA

ADMINISTRATION OFFICE
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

TAB D

1. The mission of the General Cryptanalytic Branch Administration Office is the administration and technical control of the operations of the branch.

2. Organization.

a. This group is organized into two distinct elements - administrative and technical, as illustrated on the organizational chart, attached as Inclosure 1.

b. The functions of the Administrative Unit are as follows:

(1) Supervision of mails, filing and records.

(2) Control and direction of personnel.

(3) Registration, storing, and distribution of documents.

c. The functions of the Technical Unit are as follows:

(1) Planning and Priorities.

(a) To direct or prepare special studies of the work in the General Cryptanalytic Branch relating to traffic intercept and coverage and traffic types as required by higher echelons.

(b) To integrate the work of the various sections in the General Cryptanalytic Branch and the General Analysis Section of Traffic Analysis and Control Branch in studies of intercept coverage and in the preparation of priorities for intercept targets.

(c) To establish the cryptanalytic intercept priorities for all diplomatic and commercial traffic.

(d) To maintain general supervision over the distribution of non-Japanese military traffic, making identification of such traffic as cannot be readily identified.

(e) To maintain general supervision over the activities of the indexing units of the General Cryptanalytic Branch for the purpose of insuring that maximum advantage is taken of the information contained in the logs.

(f) To compile and maintain the list of trigraphic designations.

(g) To supervise the preparation and study of the monthly system reports.

(h) To maintain daily contact with all operating sections of the General Cryptanalytic Branch to determine what traffic or collateral information may be valuable to them in their work and to find such material and bring it to their information.

(i) To inform all units of operations being performed by others which could increase their own efficiency.

(j) To make recommendations, based on the information obtained in the performance of the above duties, to the Chief, General Cryptanalytic Branch, concerning improvements in efficiency of operations or the employment of personnel.

(k) To coordinate cryptanalytic needs for traffic with the British Exchange Unit and to establish forwarding priorities of wire traffic from the Cable Censor.

(2) Recorder's Unit.

(a) Within Branch.

1. The preparation of technical papers which deal with the theory and application of cryptanalytic methods.

2. The preparation of papers dealing with the cryptanalysis of specific systems describing their cryptography, history, methods of cryptanalysis, their relation to other systems, and the materials necessary to their development and exploitation.

3. The preparation of a daily information bulletin distributed at the end of each day which records and informs higher authority of significant events of that day in the Branch.

4. The preparation of a semi-monthly report to the Commanding General.

5. The preparation of an annual report of the activities of the Branch.

6. The preparation of such historical studies as the Branch is directed to make.

7. The preparation of miscellaneous papers: surveys, summaries of cryptanalytic work done, progress reports, staff studies, liaison reports, indexes, and other such statements or records for which a need arises in the administration, operation, or liaison of the Branch.

(b) Within Division.

1. Filing of semi-monthly report of branches.

2. General supervision of the form of semi-monthly reports, annual reports, and historical studies.

(c) Committee on Terminology.

1. Publication and recording of the proceedings of the committee.

2. Continuous revision of the glossary of terms.

3. Carrying on of the committee's correspondence within the Agency and with other centers.

4. Preparation of revisions of TM 20-205 in the field for which the Signal Security Agency is responsible.

(d) For the Commanding General.

1. Preparation of a detailed study of the liaison which has been carried on between the Signal Security Agency and the London establishments of the Government Code and Cipher School.

(3) Liaison and Training Unit.

(a) This unit is concerned with the constant interchange of technical knowledge within the General Cryptanalytic Branch, with other branches, with the Navy, with the Coast Guard, with the Examination Unit, with the Government Code and Cipher School, and with the instructions of personnel in methods and procedures. It is also concerned with the study and routing of terminal documents and compromised material.

REF ID:A70871

(4) Research Section.

(a) Recommends, examines, advances, and employs profitable cryptanalytic means of attack on current problems.

(b) Maintains liaison with Equipment Branch and Cryptographic Materiel Branch in order to exchange ideas, advice, and opinions on present and proposed models of cipher machines, including cifax and ciphony.

(c) Conducts theoretical investigations into general problems connected with cipher machines.

d. The functions of the Adjutant are as follows:

(1) Serves as property officer - directs maintenance and allocation of supplies.

(2) Serves as officer of conservation, security.

(3) Serves as custodian of registered documents.

3. The Administration Office maintains liaison with the following units:

a. All sections of General Cryptanalytic Branch.

b. Intelligence Division and other branches of the division.

c. Government Code and Cipher School, Examination Unit, Navy, Coast Guard, and Military Intelligence Service.

d. Personnel Branch.

e. Supply Branch.

f. Security Division.

4. Personnel.

a. The following is a list of the personnel employed in the General Cryptanalytic Branch Administration Office:

Male Officers	- 7
WAC Officers	- 1
Enlisted Men	- 3
Enlisted WAC	- 1
Military Personnel	- 12
Civilians	- 30
Total Personnel	- 42

TOP SECRET

b. This list of personnel is adequate to perform the mission assigned.

5. Space.

a. The Administration Office is located in the headhouse of Wing 2, first floor, Operations "B", and in Wing 3, Operations "D". A floor plan of this section is attached as Inclosure 2.

b. This space is not adequate because several units within the Administration Office are located away from the main office in the headhouse. Then too, there is not enough space in the headhouse to adequately house the personnel assigned.

c. This location is not convenient for work and contact with the various sections of the General Cryptanalytic Branch, particularly the ones located in Operations "A". Because of this, the mail system is very complex, and many times important material, which is sent through the mail, is delayed.

6. The lighting is not adequate.

7. Files.

a. The following files are maintained in this section:

(1) Document files.

(2) Administrative files.

(3) Telegrams.

b. It is believed necessary to maintain a file of documents similar to that maintained in the Information Section of Information and Liaison Branch, because the personnel of the Documents Unit are not sufficiently qualified technically nor in close enough contact with the operating units to perform a detailed job of cross reference and distribution of documents. The existence of the Documents Unit has saved a great deal of time because of the close liaison maintained between this unit and the operating sections.

c. Because of the highly classified material used for reference by the sections of the General Cryptanalytic Branch, many documents do not go through the Information Section of Information and Liaison Branch - these documents are directed to the Document Unit of General Cryptanalytic Branch.

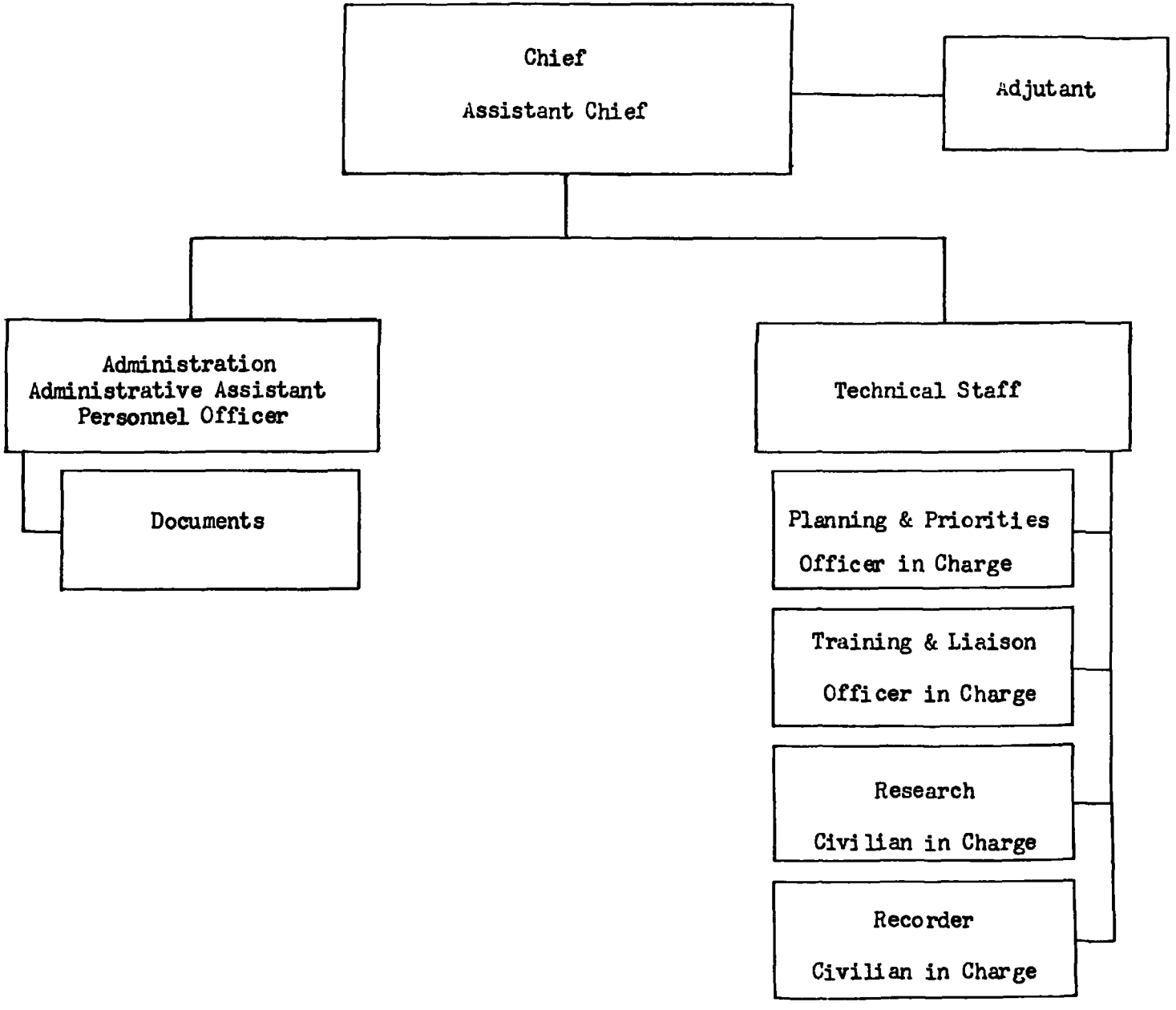
2 Incls
1. Org Chart - Adm Off
2. Floor Plan - Adm Off

TOP SECRET

REF ID:A70871

ADMINISTRATION ~~SECRET~~

GENERAL CRYPTANALYTIC BRANCH, SPSIB-3



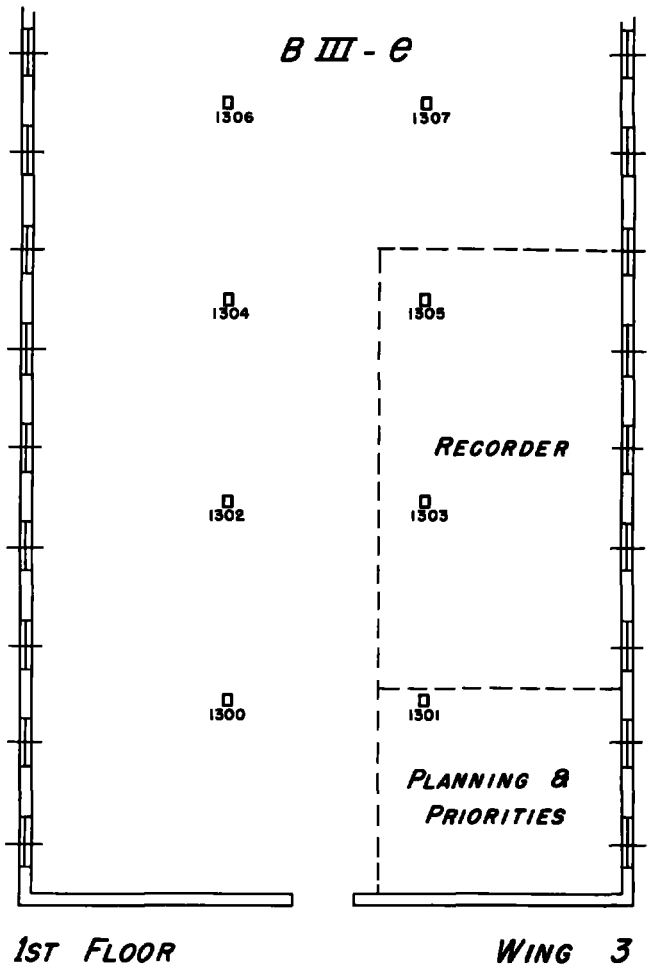
~~SECRET~~

REF ID:A70871

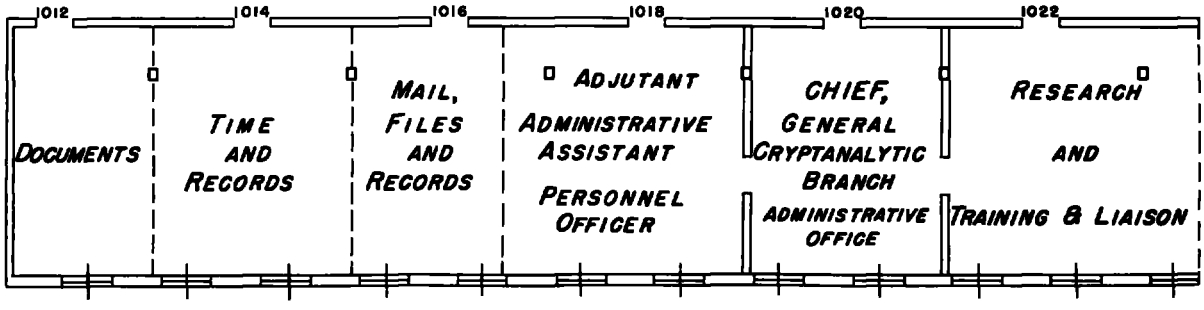
ADMINISTRATIVE OFFICE

GENERAL CRYPTANALYTIC BRANCH

SPSIB - III



OPERATIONS "B"



HEAD HOUSE – OPPOSITE WINGS 1 AND 2

1ST FLOOR

SPSIS-IA

REF ID:A70871

ROMANCE LANGUAGES SECTION, SPSIB-3A
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the Romance Languages Section is the research, development and exploitation of two hundred diplomatic and miscellaneous systems from twenty-five governments using seven diffprent languages.

2. This section is organized into seven subsections, as illustrated on the organizational chart, Inclosure 1. The work flow of each of these subsections follows generally the typical example set forth in Tab B.

TAB E

3. The Romance Languages Section maintains liaison with the following sections:

a. Bulletin Section of Information and Liaison Branch.

b. Military Intelligence Service.

c. Traffic Analysis and Control Branch.

d. General Machine Cipher Section of General Cryptanalytic Branch.

e. Miscellaneous Diplomatic Section of General Cryptanalytic Branch.

f. Government Code and Cipher School.

g. Machine Branch.

h. Laboratory Branch.

4. Personnel.

a. The following is a list of the personnel engaged in work in this section:

Male Officers	- 6
WAC Officers	- 1
Enlisted Men	- 0
Enlisted WAC	- 8
Military Personnel	- 15
Civilians	-178
Total Personnel	-193

b. The present personnel is not adequate to properly perform the mission of the section. Additional skilled cryptanalysts are needed. This personnel has been requisitioned from the Personnel and Training Division.

TOP SECRET

c. There is considerable dissatisfaction among the personnel in this section. A more than usual number of employees in this section have been in the section for several years and cannot be raised in grade any further. There is also the fact that many employees believe that there is no post-war future to their work, and therefore feel that there is little security to their jobs.

5. Space.

a. The Romance Languages Section is located in the 8th wing, second floor, Operations "A". A floor plan of this section is attached as Inclosure 2. This location is not too convenient for contact with other sections.

b. The space in this section is not adequate. It would be beneficial to have the administrative office of this section segregated from the rest of the section, because of the privacy necessary for personnel and administrative work.

6. The lighting in the Romance Languages Section is adequate, as this section is located in an end wing.

7. Files.

a. The following files are maintained in the Romance Languages Section:

(1) Old and current traffic.

(2) Collateral code and reference books.

(3) Correspondence and other administrative files, including documents and technical write-ups.

b. These files are maintained for a year, as a maximum time. The length of time varies with the research and use of the material.

8. The following reports are rendered by this section:

a. Daily technical progress reports for the Daily Information Bulletin.

b. Monthly system surveys - submitted to Trends Research Unit.

c. Miscellaneous personnel reports - submitted to General Cryptanalytic Branch.

9. The following material is used as reference material:

a. Message logs - maintained for 2 years.

b. "D" Summaries - maintained for 3 months.

c. Project 900 - maintained since the beginning of this project.

d. Dictionaries.

e. Old traffic - maintained 2 to 3 years.

f. Material and information obtained from the Information and Liaison Branch.

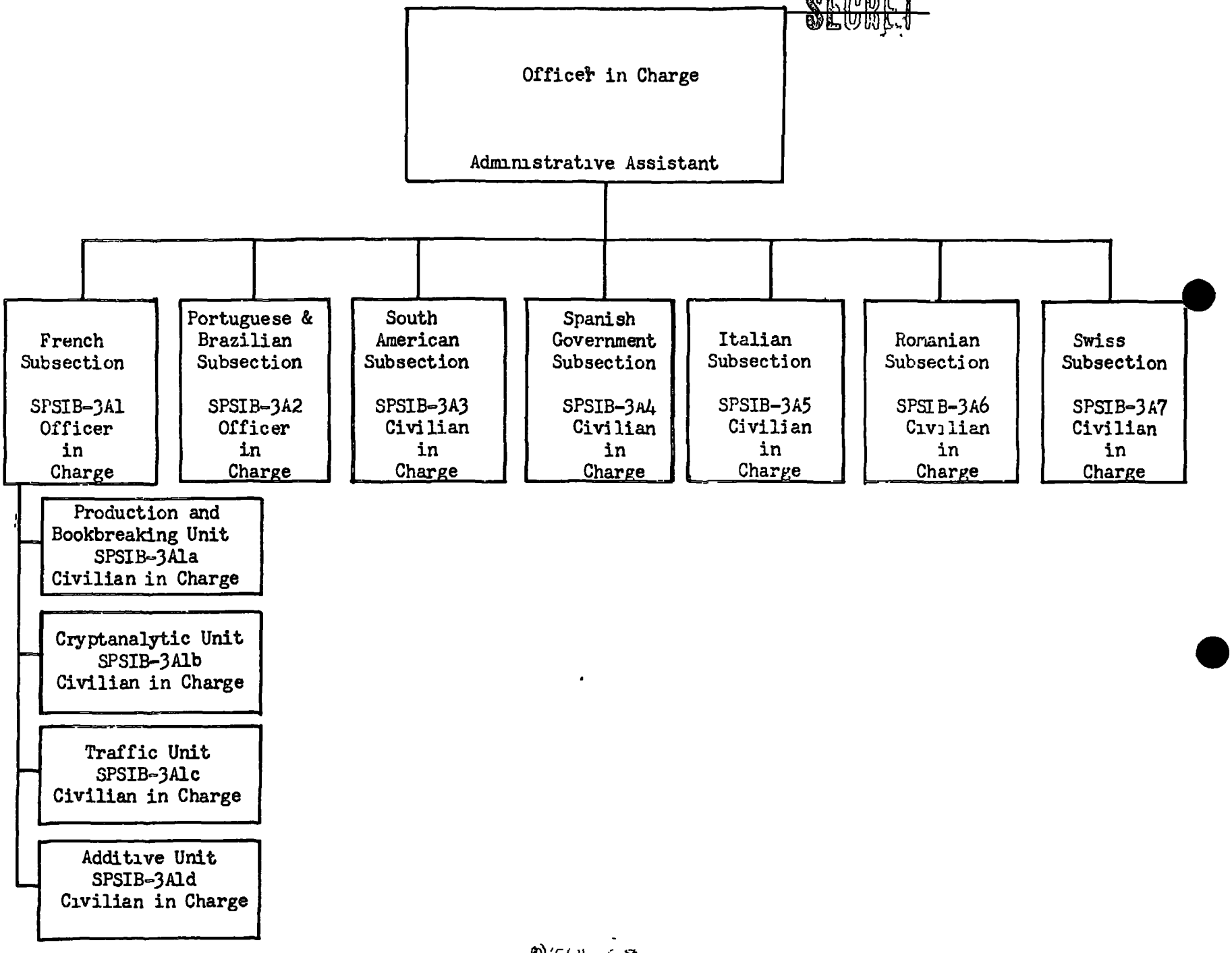
2 Incls
1. Org chart - SPSIB-3A
2. Floor plan - SPSIB-3A

TOP SECRET

REF ID:A70871

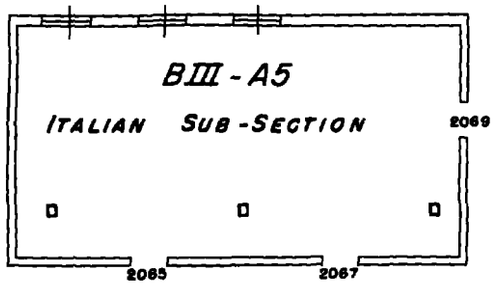
ROMANCE LANGUAGE SECTION SPSIB-3A

SECRET



SECRET

REF ID:A70871



HEAD HOUSE – ADJOINING WING 7
2ND FLOOR

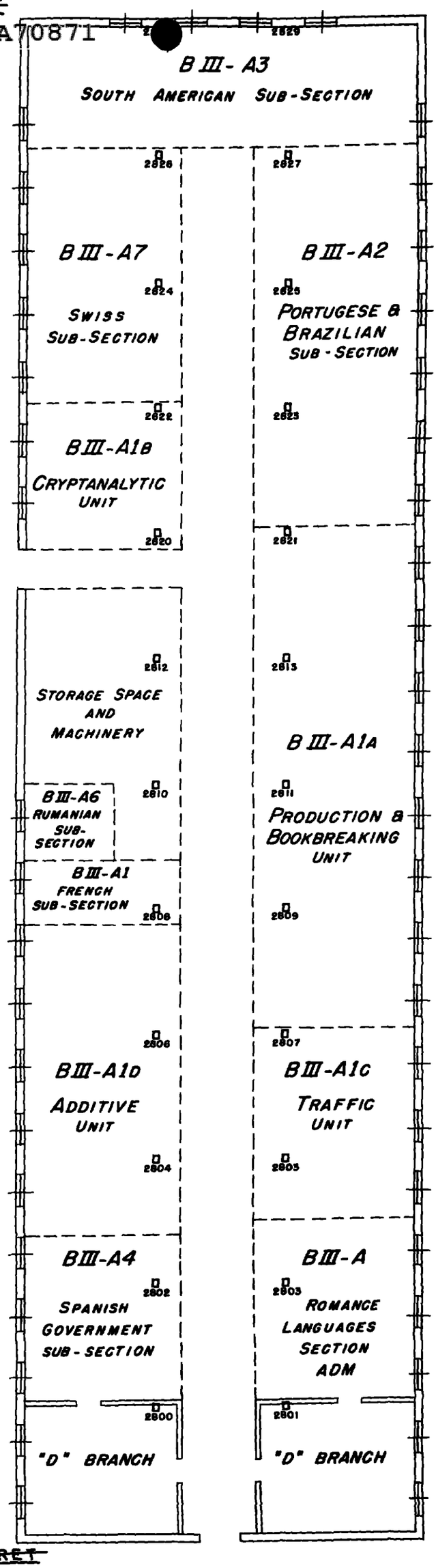
ROMANCE LANGUAGES SECTION

GENERAL CRYPTANALYTIC BRANCH

SPSIB-IIIA

OPERATIONS "A"

WING 7
2ND FLOOR



REF ID:A70871

COMMERCIAL SECTION, SPSIB-3B
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. Historical Background.

a. In January of 1944, the Signal Security Agency was required by law to accept in its quota of new personnel a certain percentage of negro personnel. The majority of the negro personnel hired were of low grade and best suited to manual labor in Cryptographic Material Branch, Machine Branch, and to do custodial work. There were contained in the groups, however, persons of good educational background and a high degree of intelligence who were not suited to manual labor and who could be gainfully employed in technical operations. Because of the large percentage of Southerners employed in the Agency it was decided that friction could be avoided if the negro personnel could be set up in a separate section and given a special job to do. At that time the only job which could be assigned as a unit and which would fit the state of the training of the personnel was the handling of commercial and public codes. The unit was consequently organized with the mission of decoding messages in commercial and public codes and studying commercial messages in unknown codes for the purpose of identifying the code book used.

TAB F

b. This unit was attached to the headquarters of "B" Branch under the staff supervision of B-3. In October, 1944, the section was attached administratively to the General Cryptanalytic Branch. As time passed, more personnel with linguistic ability were added, and those on the job grew more familiar with cryptanalytic techniques. Therefore, to keep pace with this growth in technical proficiency, new jobs were assigned to this section. These jobs have included the scanning of commercial and private plain text with the object of choosing messages which might have intelligence value; the research and development of the diplomatic traffic of several of the lesser important countries; and most recently, the decoding of a low-grade Japanese diplomatic system.

2. The mission of the Commercial Section is the identification and exploitation of commercial codes used by commercial houses in various countries throughout the world and the examination of commercial plain text for intelligence; the solution and exploitation of diplomatic traffic of Belgium, Luxembourg, Haiti, and Liberia; the decoding of traffic in the low-grade Japanese diplomatic system, JAH.

3. This section is organized into six subsections, as illustrated on the organizational chart, Inclosure 1.

4. The Commercial Section maintains close liaison with the following sections:

a. The Machine Branch.

b. The Information and Bulletin Sections of Information and Liaison Branch.

TOP SECRET

c. The Japanese Diplomatic Section of the General Cryptanalytic Branch.

d. The Japanese Diplomatic Translation Section of the Language Branch.

5. Personnel.

a. The following is a list of the personnel employed in the Commercial Section:

Male Officers - 1
Civilians - 33

Total Personnel - 34

b. The above personnel is adequate to perform the mission assigned.

c. There is the usual dissatisfaction in this section due to lack of promotions.

d. The personnel work on the day and swing shifts, although it is generally believed by the Officer in Charge and the personnel of the section that the swing shift is very inefficient.

6. Space. The Commercial Section is located in the headhouse adjoining the first wing, first floor, Operations "B", and an additional room in the headhouse between the first and second wing. A floor plan of this section is attached as Inclosure 2. The space assigned to the section is inadequate and results in the necessity for a swing shift. The operation of a swing shift on a problem which is as small as this and which calls for close team work among the personnel is wasteful of the time and money of the government. Many problems, both technical and with regard to personnel, have arisen as a result of the operation of this shift.

7. The lighting is considered completely inadequate as has also been expressed in other sections.

8. Files.

a. The following files are maintained in the Commercial Section:

(1) OAA decodes and undecoded messages.

(2) Duplicate messages of JAH.

(3) Index card file of collateral information.

b. The time that any material is kept varies with its importance, but all material is kept for a minimum of 90 days.

9. The following reports are rendered by the Commercial Section:

a. System Report - to Trends Research Unit of Control Office.

b. Progress Report - to Recorder of General Cryptanalytic Branch.

c. Miscellaneous personnel reports - to Personnel Officer of General Cryptanalytic Branch.

10. The reference material used by the Commercial Section consists of information files, and certain other available publications.

11. Organization and Work Flow.

a. A clear understanding of the organization of the Commercial Section and the flow of work through this section can best be obtained if the several distinct functions are examined separately. These functions are:

(1) The decoding of messages in commercial and public codes.

(2) The scanning of commercial and personal plain text.

(3) The research, development, and exploitation of the diplomatic traffic of Belgium, Luxembourg, Haiti, and Liberia.

(4) The decoding of messages in the Japanese Diplomatic system, JAH.

b. Traffic in Commercial and Public codes (arbitrarily called by the trigraph QAA) is received in the Commercial Section from the Records and Distribution Subsection of the Traffic Analysis and Control Branch, through the Traffic Unit of the Intelligence Division. The traffic is sorted in the Files and Records Subsection on the basis of the countries from and to, in general categories, e.g:

(1) Enemy to Enemy

(2) Neutral to Neutral

(3) Enemy to Neutral

(4) Neutral to enemy

(5) Allies to Neutral

(6) Neutral to Allies

This sort is used as a tool to decide the order of decoding the messages, priority being given the first four categories listed above.

c. The traffic is then indexed in a book with the major sort being on the date received in the section and the following pertinent information listed:

(1) City from and City to

(2) Date of the Message

(3) The Code Book Used

(4) Addressee

(5) Originator

(6) Identifying Code Groups

The indexer uses her spare time to study messages in which the code is not immediately recognizable, comparing the code groups against a set of permutation tables of all known commercial code books. If it should be impossible to determine the code book the traffic is placed in a file of unidentified messages. There is not a very large volume of messages in code books which are unknown.

d. The messages are then turned over to the Decoding Subsection where they are decoded in accordance with the general precedence scale set forth above.

e. From the Decoding Subsection the messages are passed to the editor of the Commercial Intelligence Bulletin. The editor scans the decodes to determine which messages are of sufficient value to be run in the Commercial Bulletin. Messages which are rejected are filed permanently, while those of some value are combined with the commercial plain text messages to constitute the Commercial Bulletin. (For more complete description of the Bulletin, see paragraph 11 i.)

f. There were some minor inefficiencies and duplication of effort in the processing and filing of this traffic, which were called to the attention of the Officer in Charge and which are being examined by him with a view to correction.

g. All plain text traffic (except Japanese) which does not have easily recognizable diplomatic addresses is sent to the Commercial Section of the General Cryptanalytic Branch. It is received in the section in the same manner as the commercial code traffic described above. The traffic is first counted in bulk. It is then given to several translators who sort it by language. These translators are able to distinguish German, French, Spanish, Portuguese, and Italian. Messages in all other languages are placed in a file of miscellaneous messages.

h. The messages in each language are then given to the translator who specializes in that language for scanning. The translator picks out messages which may be diplomatic in nature, although not easily recognizable in external appearance, and sends these messages to the appropriate section in the General Cryptanalytic Branch; he separates and destroys the purely personal plain text and chooses from the commercial plain text messages which are liable to be of value. These last are passed on to the Commercial Bulletin editor. The messages labeled miscellaneous are sorted by the principal translator, who is able to recognize the language. By certain minimum standards (such as the knowledge of the words for ton, bill of lading, shipping, love and kisses, etc.) these messages are scanned and as many personal and commercial messages as is possible are sorted out. Those which cannot be recognized by these standards are then sent to the appropriate language section of the General Cryptanalytic Branch for classification. They are then returned to the Commercial Section. The personal messages are destroyed on the spot. The general run of commercial messages are counted, the intercept preambles cut off, and sent to the Military Intelligence Service, through the Bulletin Section of the Information and Liaison Branch, for forwarding to the Foreign Economics Administrator. The commercial messages which are chosen as having some possible intelligence value are passed to the editor of the Commercial Intelligence Bulletin.

i. The Commercial Intelligence Bulletin is a special publication issued weekly which contains only messages processed in the Commercial Section. Included in this Bulletin are commercial messages from both code and plain text which are presumed to have some value to Military Intelligence. The stencils for this Bulletin are prepared in the Commercial Section and the stencils are sent to the Bulletin Section of the Information and Liaison Branch for duplication.

j. The Cryptanalytic Subsection of the Commercial Section does research, development, and exploitation of the traffic of Luxembourg, Haiti, Belgium, and Liberia. In the processing of this traffic, the subsection is organized in a manner identical to that described in the survey of the Romance Language Section, and it is not believed that a more detailed description is necessary.

k. The processing of Japanese Diplomatic traffic in the system JAH is handled by the subsection of this section. The messages are received with a cover sheet attached on which is written significant data such as the city to city circuit, the message number, message part number, relay groups, date, etc. This subsection performs two different processes on this traffic:

(1) Intercepts which are good solid copy are edited for IBM processing and sent to the Machine Branch for machine decoding.

TOP SECRET

(2) Intercepts which are garbled are decoded by hand.

1. After a message has been decoded either by hand or machine, all parts of the message are assembled and the message passed to the Japanese Diplomatic Translation Section of the Language Branch, from which point it is processed as is any other Japanese diplomatic message.

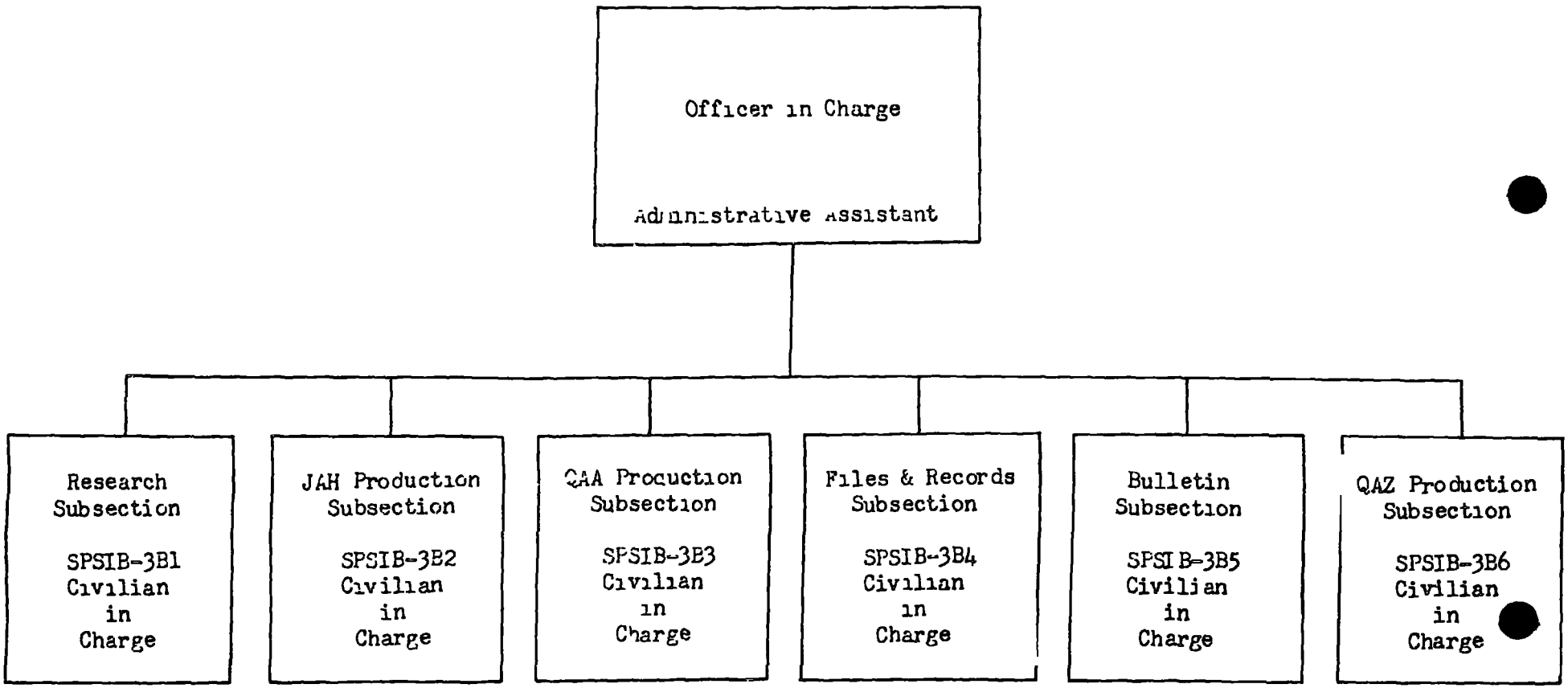
2 Incls
1. Org Chart - SPSIB-3B
2. Floor Plan - SPSIB-3B

REF ID:A70871

~~SECRET~~

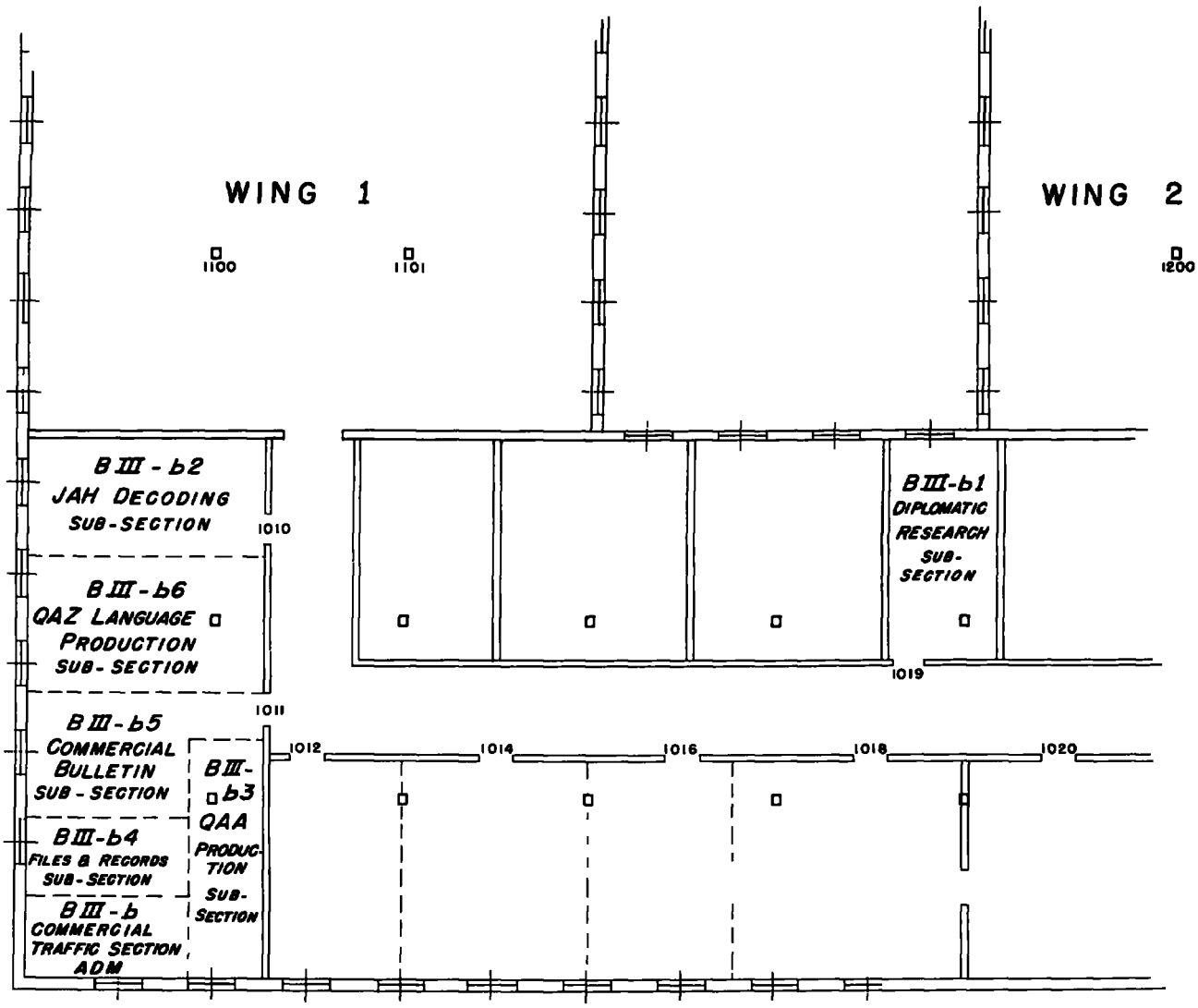
COMMERCIAL TRAFFIC SECTION

SPSIB-3B



~~SECRET~~

REF ID:A70871



HEAD HOUSE 1ST FLOOR

OPERATIONS "B"

COMMERCIAL TRAFFIC SECTION

GENERAL CRYPTANALYTIC BRANCH

SPSIB - III b

GENERAL MACHINE CIPHER SECTION, SPSIB-3C
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the General Machine Cipher Section is the cryptanalysis and research on machine cipher systems and operation and maintenance of cryptanalytic machinery.

2. The General Machine Cipher Section is made up of five subsections, as illustrated on the organizational chart, attached as Inclosure 1, with duties as follows:

a. Operation and maintenance of photo electronic cryptanalytic machinery, (RAM).

b. Cryptanalysis and research on electrical machine ciphers and related systems.

c. Cryptanalysis and research on mechanical machine ciphers and related systems.

TAB G

d. Operation and maintenance of "003" and associated equipment.

3. The following are the units with which the General Machine Cipher Section maintains close liaison:

a. Romance Languages Section - translation work on Swiss messages in German and French, and general coordination of systems worked on or being investigated for machine cipher.

b. Military Cryptanalytic Branch, Communications Security Branch, the Navy, and all sections of General Cryptanalytic Branch - use of RAM equipment.

c. Communications Security Branch and Navy - use of "003" equipment.

d. Equipment Branch - development of ideas for cryptanalytic machinery.

e. General Cryptanalytic Branch Research Staff.

4. Personnel.

a. The following is a list of the personnel employed in the General Machine Cipher Section:

Male officers	- 13
WAC Officers	- 2
Enlisted Men	- 14
Enlisted WAC	- 34
Military Personnel	- 63
Civilians	- 53
Total Personnel	116

b. The above personnel are not adequate to perform the assigned mission. Additional mathematicians and engineers are needed to be trained to become expert cryptanalysts. This additional personnel has been requisitioned.

5. The General Machine Cipher Section is located in the basement, Wing 1 and 2, Operations "B". The space allotted to this section is adequate, and the location is convenient for contact with other units. A floor plan is attached as Inclosure 2.

6. The lighting in the General Machine Cipher Section is adequate.

7. Files.

a. The following files are maintained in this section:

(1) Traffic in process.

(2) File of special parts to equipment.

(3) Traffic and worksheets - SZD, FISH, NEA, SWA, FIA, NOA.

(4) Reports and bulletins.

(5) Blue prints, machines, spare parts, etc.

b. The length of time that this material is kept depends upon the systems involved.

c. The following functions and records have been discontinued within the last six months:

(1) Logs on NOA.

(2) "003" activities.

8. The following reports are rendered by the General Machine Cipher Section:

a. Semi-monthly RAM report to General Cryptanalytic Branch and Recorder Unit.

b. Semi-monthly summary reports to General Cryptanalytic Branch and Recorder Unit.

c. Special reports on systems with new developments.

d. Strength report - weekly and monthly.

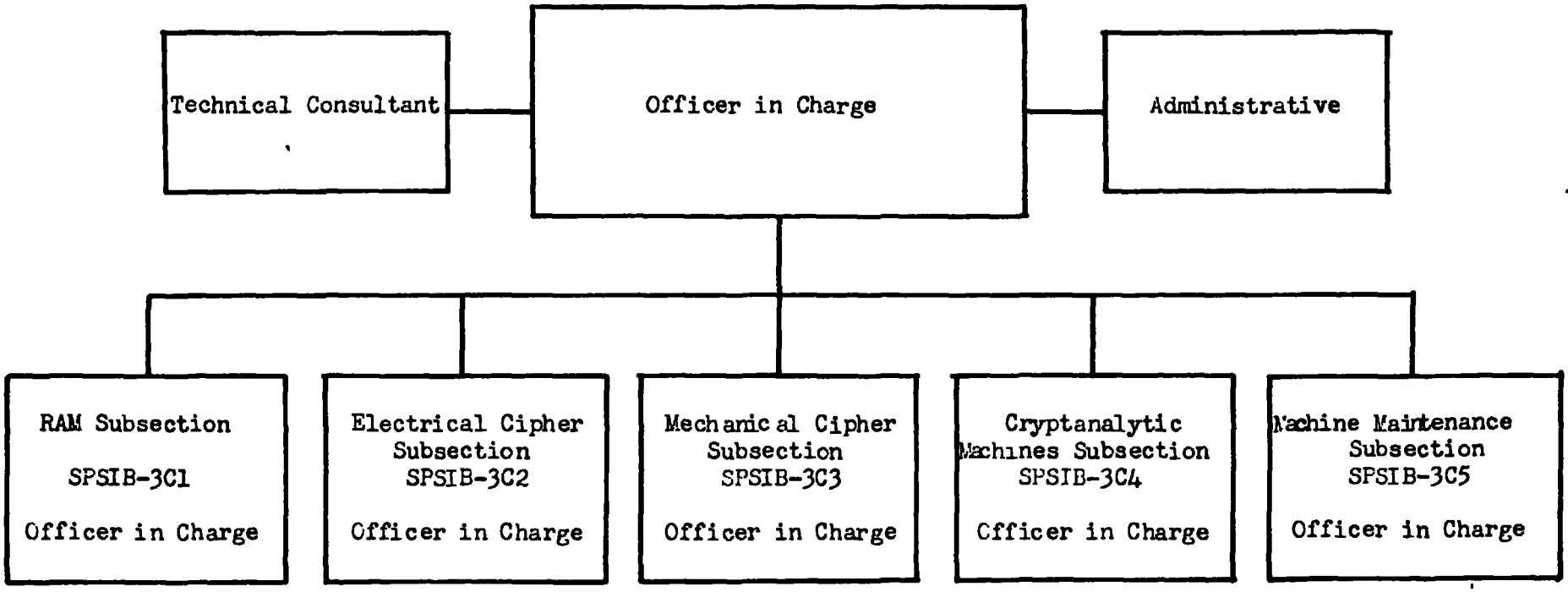
e. Monthly reports on enlisted personnel.

9. Reference material in this section consists of machines and equipment - captured or purchased - plus liaison and systems reports which are furnished by the Documents Subsection of Information and Liaison Branch. All of this material is kept on hand indefinitely.

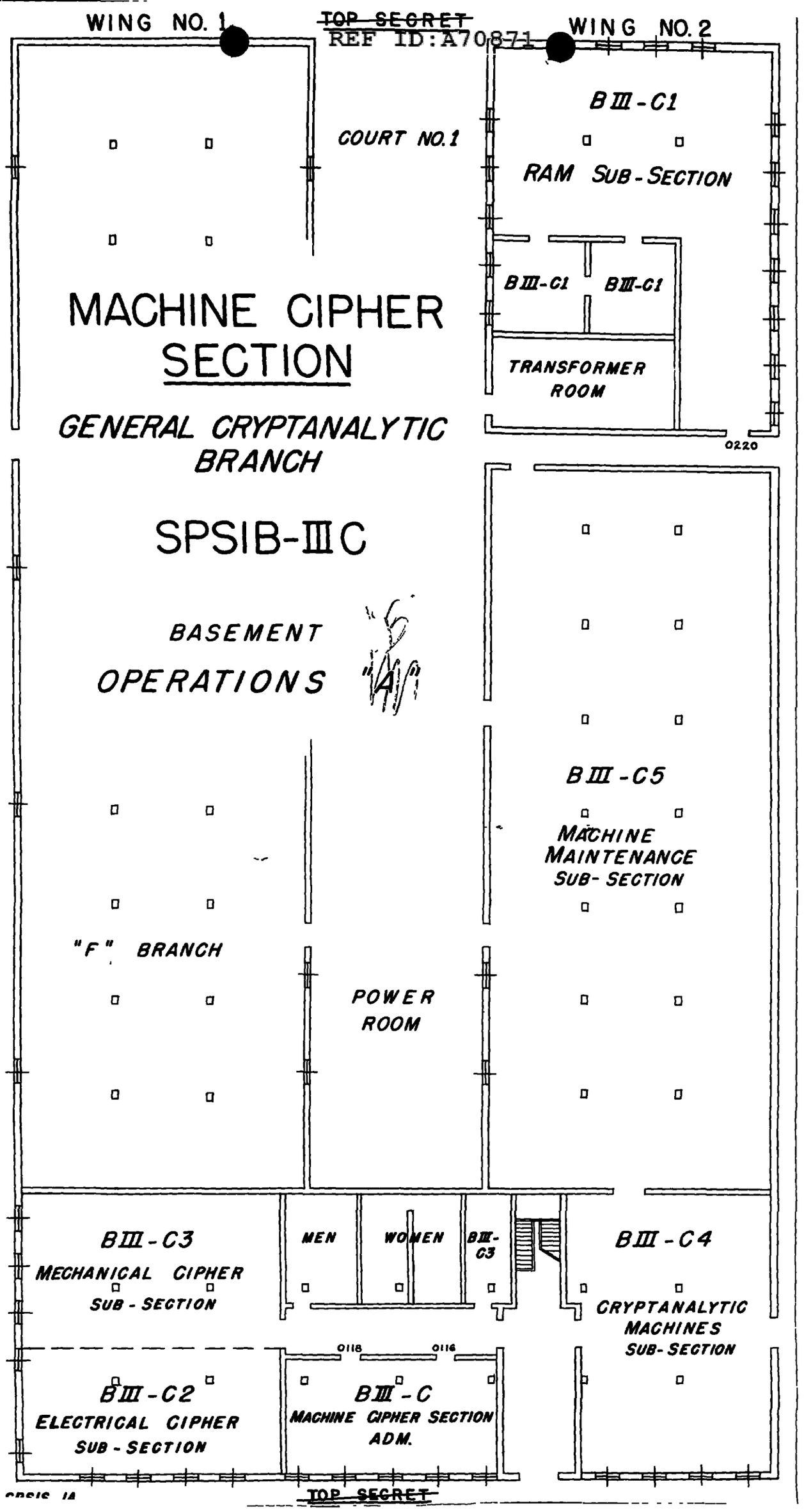
2 Incls
1. Org Chart - SPSIB-3C
2. Floor Plan - SPSIB-3C

REF ID:A70871

GENERAL MACHINE CIPHER SECTION, SPSIB-3C



~~TOP SECRET~~
REF ID:A70871



~~TOP SECRET~~

REF ID:A70871

MISCELLANEOUS DIPLOMATIC SECTION, SPSIB-3D
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the Miscellaneous Diplomatic Section is the solution, exploitation and translation of all miscellaneous diplomatic traffic, exclusive of the Japanese Diplomatic and Romance Languages traffic.

2. This section is divided into four subsections, which, in turn, are separated into units, as illustrated on the organizational chart attached as Inclosure 1.

3. The Miscellaneous Diplomatic Section maintains liaison with the following units:

a. General Analysis Section, Traffic Analysis and Control Branch.

b. OP-20-G.

c. Government Code and Cipher School.

d. Signal Intelligence Service, India-Burma Theatre.

4. Personnel.

a. The following is a list of the number of personnel employed in the Miscellaneous Diplomatic Section:

Male Officers	- 9
WAC Officers	- 2
Enlisted Men	- 7
Enlisted WAC	- 21
Military Personnel	- 39
Civilians	-160
Total Personnel	-199

b. This personnel is not adequate to perform the mission assigned to the section. People with linguistic, mathematical, and good cryptanalytic abilities are required in order to perform the mission adequately. Personnel with linguistic training have been particularly requested of the Personnel and Training Division. The requests for clerical personnel have been filled.

c. There is the usual amount of dissatisfaction in this section, due to the fact that because of Civil Service standards, good personnel cannot be promoted to higher allocated jobs, despite their demonstrated ability.

TOP SECRET

5. The Miscellaneous Diplomatic Section is located in the 7th wing, second floor, Operations "A". A floor plan of this section is attached as Inclosure 2. The space in this section is adequate, and the location is convenient for work with other sections, as most of the liaison can be carried on by means of the telephone.

6. The lighting is not adequate - additional wall outlets are needed to accommodate all of the desk lamps. The overhead lighting is inadequate, and many people complain of eyestrain.

7. The functions of the various sections of the Miscellaneous Diplomatic Section are as follows:

a. German Diplomatic Subsection, SPSIB-3D1.

(1) Translation and Records Unit, SPSIB-3D1A.

(a) Translation of all messages in GEF and GEC, plus some GEZ.

(b) Solution of messages in GEC.

(c) Maintenance of all records pertinent to translation, aid to translation, and historical files and records.

(2) Traffic Unit, SPSIB-3D1B.

(a) Receiving and sorting of all incoming traffic.

(b) Logging of all traffic.

(c) Editing of traffic for IBM processing.

(d) Maintenance of traffic files and records.

(3) Placement and Decoding Unit, SPSIB-3D1C.

(a) Placement of pad sheets of GEE for overlapping.

(b) Conducting of research relative to development of new areas and advancement of work in the subsection.

(c) Hand decoding of deciphered GEE messages.

(4) Overlap Unit, SPSIB-3D1D.

(a) Solving of GEE pads set in depth after they have been placed by the Placement and Decoding Unit.

TOP SECRET

(5) Special Examination Unit, SPSIB-3D1E.

(a) Examination of mail from United States soldiers, civilians, prisoners of war, etc., suspected by censorship, of hidden messages.

(b) Examination of messages and notes in various types of ordinary and cryptic shorthand for concealed meanings.

(c) Listening to and translating recordings of radio telephone conversations and other non-Morse recordings for material of intelligence value.

b. Miscellaneous Diplomatic Subsection, SPSIB-3D2.

(1) Far Eastern Unit, SPSIB-3D2A. This unit consists of two subunits - Chungking Government and Nanking Government. The Far Eastern Unit is responsible for the solution, exploitation of traffic emanating from the foregoing governments, plus the solution and exploitation of Thai traffic.

(2) Balkan and Central European Unit, SPSIB-3D2B. This unit is divided into the Greek, Jugoslav, Bulgarian, Czechoslovak subunits. Each of these units is responsible for the solution, exploitation, and bookbreaking of the traffic from the foregoing countries.

(3) Polish Unit, SPSIB-3D2C. This unit is responsible for general research on, solution, bookbreaking, and exploitation of Polish diplomatic traffic.

(4) Cryptanalytic Unit, SPSIB-3D2D. This unit is responsible for the research towards solution of systems normally handled by SPSIB-3D2A, SPSIB-3D2B, SPSIB-3D2C.

c. Near Eastern Subsection, SPSIB-3D3.

(1) Turkish Unit, SPSIB-3D3A. This unit is responsible for the research toward solution on new systems not yet solved. The Turkish Unit also deciphers, decodes, and translates messages in a number of readable systems and forwards results to the Bulletin Section of Information and Liaison Branch.

(2) Iranian and Afghan Unit, SPSIB-3D3B. This unit has the same function as the Turkish Unit, except that it works on Iranian and Afghan traffic.

TOP SECRET

(3) Miscellaneous Arabic and Ethiopian Unit, OPSIB-3D3G. This unit works on traffic from all of the Arabian and Levantine States, using Arabic as a vehicle of communication - also Ethiopian traffic using English, French and Abamric.

d. Weather Subsection, OPSIB-3D4. Active research on weather systems is not carried on. Liaison is effected with the Navy, Signal Intelligence Service, India-Burma Theatre, Central Bureau Brisbane, Army Air Forces Weather Central.

8. Files.

a. The following files are maintained in the various subsections:

(1) German Diplomatic Subsection:

(a) Original translations produced by subsection.

(b) Bulletin copies of translations.

(c) Translations of messages intercepted and read by the United States Coast Guard from German sources, mainly Clandestine.

(d) Traffic files, current and old.

(e) Overlap files.

(f) Suspense files for messages in translation.

(g) Record of translations completed, showing disposition and bulletin series.

(h) IBM solution runs.

(i) Documents and collateral information.

(j) Radio telephone and other voice recordings.

(k) Special examination work problems, letters, etc.

(2) Miscellaneous Diplomatic Subsection.

(a) Traffic files.

(b) Technical file of 41 numbered drawers controlled by a card index.

(3) Near Eastern Subsection.

(a) Translations

(b) Traffic.

(c) Technical write-ups and collateral information.

(d) Who's Who in the Near East.

(e) Arabic to English and English to Arabic Vocabulary on 3" x 5" index cards.

(4) Weather Subsection.

(a) Traffic files arranged by country and system.

(b) Technical.

(c) References and collateral material pertinent to weather.

(d) Correspondence pertaining to weather with agencies outside the Signal Security Agency.

b. All of the preceding files are maintained permanently, with the exception of traffic dupes, which are destroyed when their usefulness has been served, certain worksheets and IBM material - also after having served their usefulness.

9. The reports which are rendered by each subsection of the Miscellaneous Diplomatic Section are as follows:

a. Daily Information Bulletin - submitted to General Cryptanalyt Branch.

b. Semi-Monthly Technical Report - submitted to Miscellaneous Diplomatic Section.

c. Monthly Systems Report - submitted to the Control Office.

d. Miscellaneous personnel reports - submitted to General Cryptanalytic Branch.

10. The following material is kept as reference material by the Miscellaneous Diplomatic Section:

a. Secret State Department Cable Briefs - kept for 24 hours.

b. State Department Cables, Plain Text - used by translators and kept in a permanent file.

c. Project 900 - kept on permanent file.

TOP SECRET

d. Magic Summary - kept for 24 hours.

e. Miscellaneous material from the Office of Strategic Services, Military Intelligence Division, and other sources, received through the Documents Subsection in the General Cryptanalytic Branch, and retained for a short period. Used for information on material contained in messages.

f. Subsection traffic logs, indices, and processing records - kept permanently.

g. All voice recordings used in the Special Examination Unit of German Diplomatic Subsection are retained three months and then destroyed.

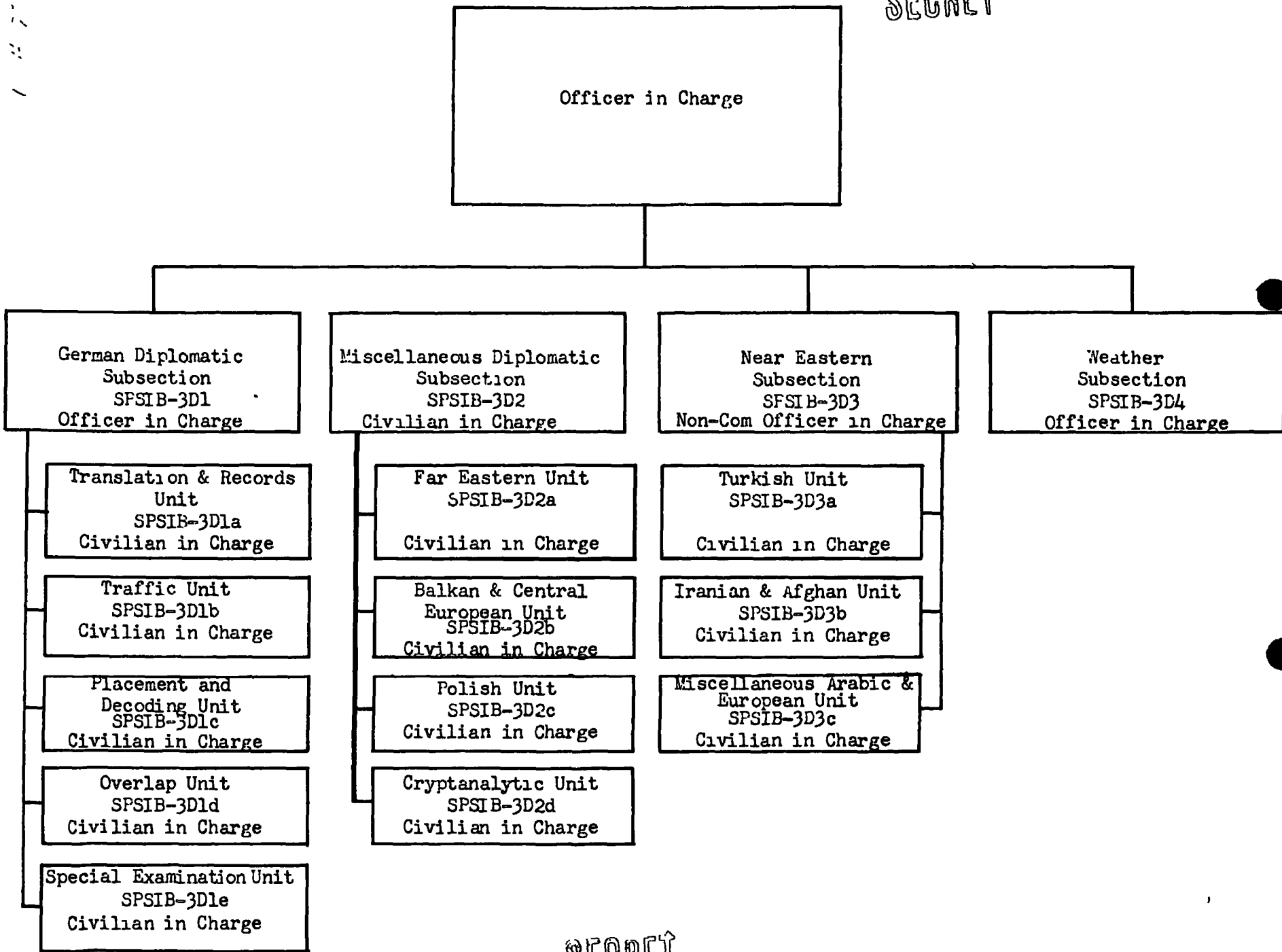
2 Incls
Org Chart, SPSIB-3D
Floor Plan, SPSIB-3D

TOP SECRET

REF ID:A70871

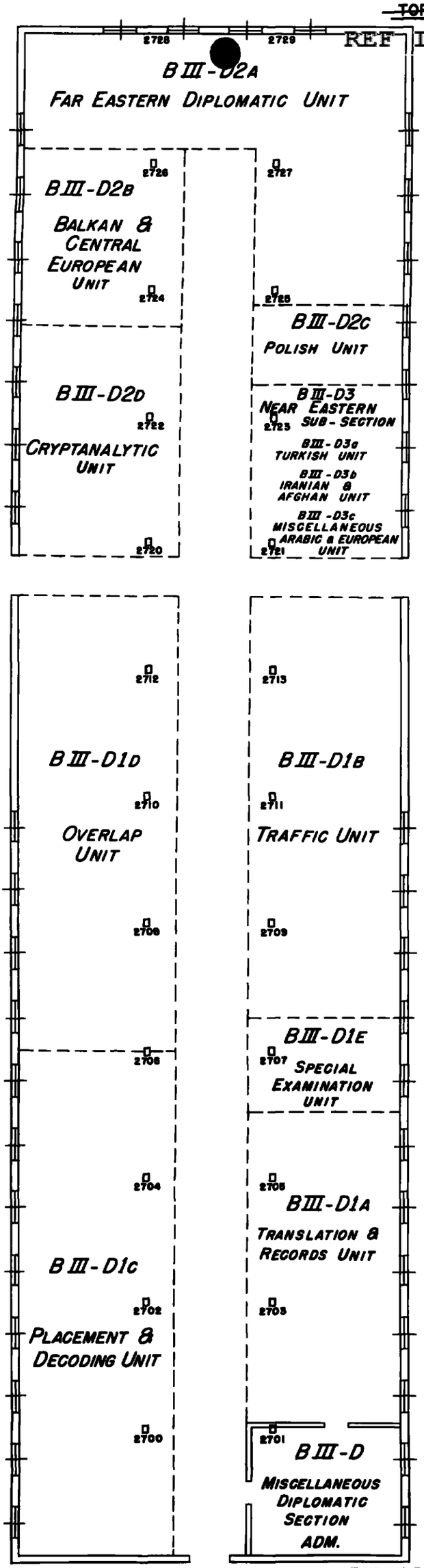
MISCELLANEOUS DIPLOMATIC SECTION SPSIB-3D

SECRET



SECRET

REF ID:A70871



MISCELLANEOUS DIPLOMATIC SECTION

GENERAL CRYPTANALYTIC BRANCH

SPSIB - III D

OPERATIONS "A"

WING 7

2ND FLOOR

SPSIS-1A

REF ID:A7087

JAPANESE MILITARY ATTACHE SECTION, SPSIB-3E
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the Japanese Military Attache Section is the research, development, and exploitation of Japanese Military Attache traffic.

2. The section is organized in six subsections, as illustrated on the organizational chart attached as Inclosure 1. The functions of each of these subsections are described below in the discussion of the work flow.

3. The Japanese Military Attache Section maintains close liaison with the Japanese Military Attache Translation Section of Language Branch; the Information Section of Information and Liaison Branch, which is called upon for collateral information for use in solution; and the Planning and Priorities Office of the General Cryptanalytic Branch, through which contact is established with other sections within the General Cryptanalytic Branch and the Intelligence Division. In addition, close and constant liaison has been maintained between this section and the Japanese Military Attache Section of the Government Code and Cipher School. The exchange of technical data and correspondence directly between the two operations sections has worked out to mutual advantage, and was the subject of special mention by the British representatives at a recent combined Signal Intelligence meeting.

4. Personnel.

TAB I

a. The following is a list of the number of personnel employed in the Japanese Military Attache Section:

Male Officers	1
Civilians	74
Total Personnel - 75	

b. In addition to the personnel listed above, there are attached to the problem officers and civilians of Language Branch - a total of 12 people.

c. The personnel of this section work on two shifts, second and third, although the majority of the employees are on the day shift.

d. The personnel currently assigned to this problem are adequate to execute the mission of the section.

5. Space.

a. The Japanese Military Attache Section is located in the third wing, first floor, Operations "B". The rear of the wing is occupied by

personnel of the Japanese Military Attache Translation Section, Language Branch, who work on this problem. A floor plan of the section is attached as Inclosure 2.

b. The space now allocated to the section is adequate.

6. There is no difficulty with regard to the lighting facilities in the section.

7. Files.

a. The Japanese Military Attache Section maintains the following files:

(1) Raw traffic for JAS, JAS-1, JAR, JAT, JBZ.

(2) Traffic logs for JAS, JAS-1, JAR, JAT.

(3) Overlap sheets for JAS, JAS-1, JAT.

(4) Work sheets for JAS page set-ups.

(5) IBM runs for pages currently under solution.

(6) Miscellaneous research data and records.

(7) Histories and special technical studies.

(8) Solved message indices.

(9) Collateral materials, such as Orders of Battle, information on military equipment, and a KANA index.

(10) Technical correspondence with Government Code and Cipher School and within Signal Security Agency.

(11) Administrative and personnel correspondence and data.

(12) Translations.

(13) Cryptographic tools.

(14) Technical reports.

(15) Record of message status.

(16) Cipher Machine Tapes.

b. Filed materials are destroyed whenever the status of the work makes such a destruction possible. IBM prints are salvaged regu-

larly as key is recovered. Most personnel correspondence and data are destroyed after twelve months. Recovered cryptographic materials are retained permanently.

8. Organization and Work Flow.

a. In order to obtain the best picture of the organization and work flow of the Japanese Military Attache Section, it is necessary to have a brief explanation of the technical problems with which this section is faced.

(1) The Japanese Military Attache traffic has been sent in four different cryptographic systems:

(a) JAR - a one-time pad system which is in the research stage.

(b) JA3-1 - a cryptographic system which is similar in nature to the system JAS which will be described below, but which, because its use has been limited to one circuit, has not been subject to the weaknesses which have permitted solution of JAS.

(c) JAT - an additive system employing a conversion square which was used for sending cryptographic and cryptanalytic information and in which all messages have been read.

(d) JAS - the principal Japanese Military Attache system which will be described in more detail.

(2) JAS is a system composed of a digraphic and tetragraphic code chart of which there have been three different sets; a literal running key of several hundred thousand letters, which normally changed every six months; and a conversion square of 26 26-letter random alphabets, which normally changed every 10 days. With the comparatively small volume of traffic which has been available in this system, it could be considered practically impossible of solution. Solution has been possible through the locating of cross-key and cross-system duplicate messages.

(3) The order of solution of the elements of the system is as follows:

(a) First, the conversion square must be solved.

(b) Second, the indicator system which gives the page and the position on the page from which the enciphering key begins.

TOP SECRET

(c) Third, messages must be overlapped and the running key stripped.

(d) Fourth, the code charts must be recovered.

(4) With the victory of the Allies in Europe the Japanese have had critical problems of distribution and have been unable to maintain their normal periods of change of the cryptographic materials. The work flow of the Japanese Military Attache Section is currently based on the following conditions:

(a) There are several systems in research.

(b) The basic code chart of the current JAS system is substantially complete.

(c) The conversion square of the current system is fully recovered and has been in effect for seven or eight weeks, which is far in excess of the normal period of a conversion square.

(d) The running key of the current key book is in the process of recovery.

b. The work flow of the section is then as follows:

(1) All traffic is received in the Traffic Subsection of Japanese Military Attache Section, from the Records and Distribution Section of Traffic Analysis and Control Branch, through the tube room located in the same wing as the Japanese Military Attache Section. In this subsection, pertinent data, such as the place from and to, the message number, the indicator groups, group count, and other data which is pertinent to solution or record keeping, is entered on five-way cards. These cards constitute a unique message indexing system which has been developed to serve the needs of this special problem.

(2) All traffic is then sent to the Research Subsection of the Japanese Military Attache Section. In this subsection the traffic in JAS-1 and JAR is under study and it is retained in the subsection. The indicators of messages in JAS are studied and deciphered. These messages then fall into two categories; messages which are on portions of the key which have been fully recovered, and messages which are on portions of the key which have not been recovered.

(3) Messages which fall on portions of the key which have been fully recovered are turned over to the Machine Subsection. A machine was developed for the decryptographing of this system which has saved thousands of man hours. In this machine the letters of the running key are punched up on Baudot tape and the conversion square is wired on an IBM plug board. The cipher text of the message is typed on a regular typewriter keyboard, the machine performs the conversion, and the decipherment and prints the message in plain code form.

(4) The messages which are on portions of the key not recovered are turned over to the Overlap Subsection. The Overlap Subsection places the messages on overlaps and strips the running key when sufficient depth has accumulated on any portion of the key to permit stripping.

(5) Messages which have been deciphered by either the Machine Subsection or the Overlap Subsection are then turned over to the Records Subsection, which has the responsibility of decoding the messages, preparing them for translation, and keeping the records on all messages which have been solved.

(6) The decoded messages are turned over to the translators in the Military Attache Translation Section of Language Branch for translation. In the past, all decodes were typed up in final form and all parts were correlated before being turned over to the translators. In recent months, however, the translators have been translating directly from the worksheets or overlap pages, and a small subsection of the Japanese Military Attache Section, called the Aides to Translators Subsection, has been maintained to correct garbles, correlate parts, etc., for the translators.

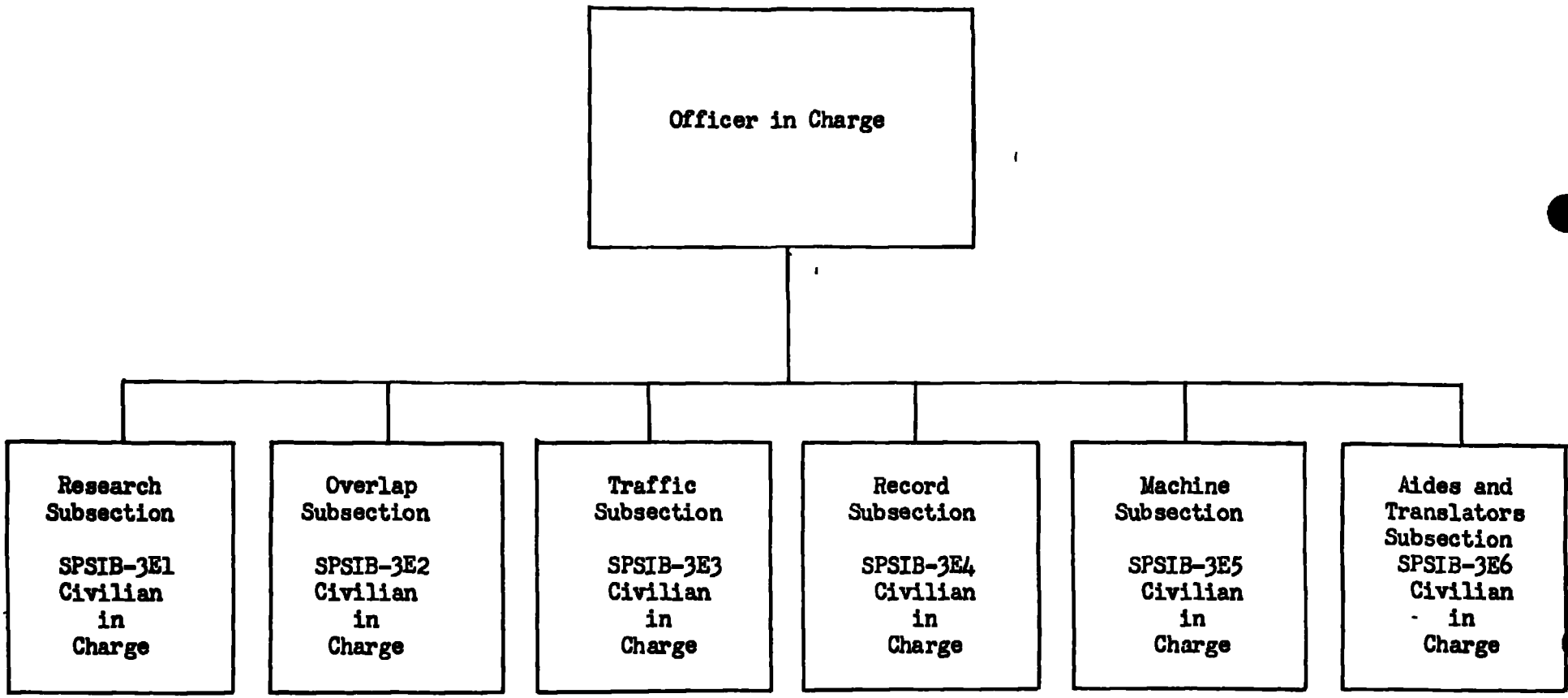
9. This section, unlike the other sections of the General Cryptanalytic Branch, has a homogeneous problem to study. The traffic being all of the Military Attache and technical problem being limited to one principal system with very few subordinate systems has permitted a simple organization which has been outstanding from the point of view of cryptanalysis and production. The fact that the section has been operating as a unit for several years has further contributed to its success. The Japanese Military Attache Section is to be commended on its organizational efficiency and its technical effectiveness.

2 Incls
1. Org. Chart - SPSIB-3E
2. Floor Plan - SPSIB-3E

REF ID:A70871

~~SECRET~~

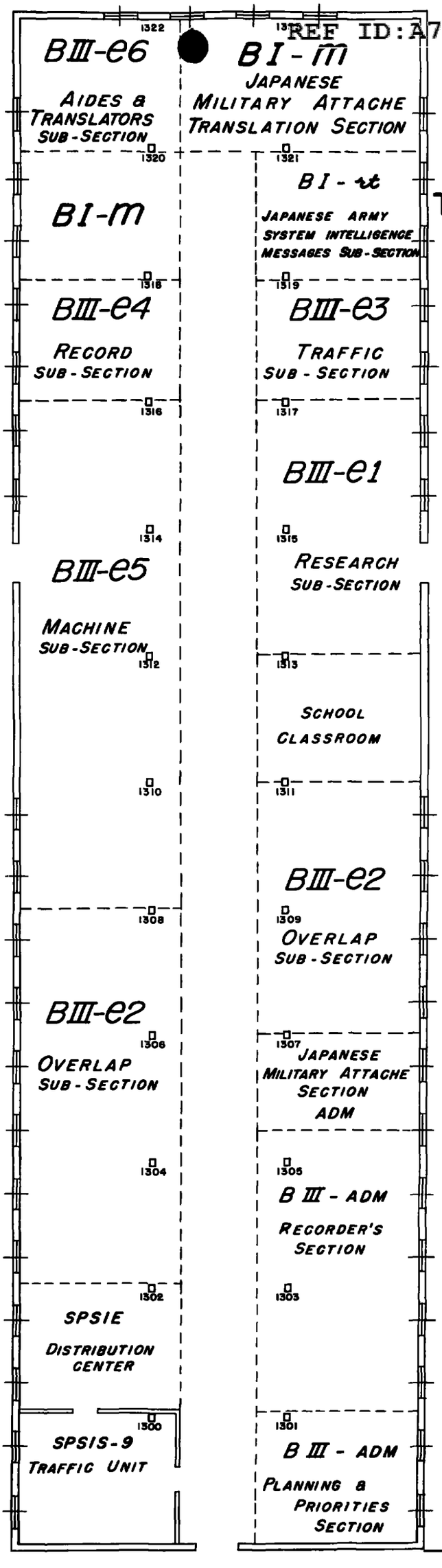
JAPANESE MILITARY ATTACHE SECTION SPSIB-3E



~~SECRET~~

TOP SECRET

REF ID:A70871



JAPANESE
MILITARY ATTACHE
TRANSLATION SECTION

LANGUAGE BRANCH

SPSIB - Im

WING 3

1ST FLOOR

OPERATIONS "B"

JAPANESE
MILITARY ATTACHE
SECTION

GENERAL CRYPTANALYTIC BRANCH

SPSIB - IIIe

SPSIS-1A

TOP SECRET

JAPANESE MILITARY ATTACHE TRANSLATION SECTION, SPSIB-1M
LANGUAGE BRANCH, SPSIB-1

1. The mission of the Japanese Military Attache Translation Section is the bookbreaking, translation and providing linguistic assistance to the cryptanalysts in the Japanese Military Attache Section of the General Cryptanalytic Branch.

2. Organization. The personnel of this section perform two major duties, translation and linguistic aid to solution of overlaps. These two functions constitute the only organizational breakdown of the work.

3. The Japanese Military Attache Translation Section maintains close liaison with:

a. The General Machine Cipher Section, General Cryptanalytic Branch.

b. Other translation sections of Language Branch.

c. The Information Section of the Information and Liaison Branch.

d. The Bulletin Section of the Information and Liaison Branch.

4. Personnel.

a. The following is a list of the personnel employed in the Japanese Military Attache Translation Section:

TAB J

Male Officers	- 2
WAC Officers	- 0
Enlisted Men	- 3
Enlisted WAC	- 0
Military Personnel	- 5
Civilians	- 7
Total Personnel	-12

b. The personnel is adequate for the mission of the section.

5. Space. The Japanese Military Attache Translation Section occupies the rear of the third wing, first floor of Operations "A" Building. See Floor Plan attached to Tab I.

6. Lighting. The lighting in the area of the wing where this section is located is adequate.

7. Files. Files of all messages which have been translated are kept in the Japanese Military Attache Translation Section.

8. Reports. The only recurring report submitted by the Japanese Military Attache Translation Section is the semi-monthly Progress Report for the Chief, Language Branch.

9. General.

a. The part played by this section in the processing of Japanese Military Attache messages is explained in the paragraph on Organization and Work Flow, Tab I.

b. One unique procedure of this section is the assignment of Bulletin numbers to translations within the section. Since a special publication series (the D Series) is set aside for Japanese Military Attache messages, the serial publication numbers are assigned to translations in this section instead of in the Bulletin Section as is the case with all other publication series.

TOP SECRET

JAPANESE DIPLOMATIC SECTION, SPSIB-3F
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the Japanese Diplomatic Section is the research, development and exploitation of Japanese cryptographic systems other than those of the Japanese Army, Japanese Navy, Japanese Military Attache, and Japanese Weather.

2. For the performance of this mission, the Japanese Diplomatic Section is organized in five subsections (see organization chart attached as Inclosure 1). The duties and responsibilities as well as the method of performance of these subsections are described in the explanation of the work flow which appears below.

3. The Japanese Diplomatic Section maintains close liaison with the following units:

a. The Commercial Section of General Cryptanalytic Branch, which performs one of the technical operations in the production of Japanese Diplomatic traffic, and which is described in greater detail in the survey of the Commercial Section.

b. The Japanese Diplomatic Translation Section of the Language Branch, which translates all messages in Japanese Diplomatic cryptographic systems. See control survey of this section.

c. The Research Subsection of the Japanese Diplomatic Translation Section, Language Branch, which is composed of several Japanese linguists who work in the same wing as the cryptanalytic units, lending linguistic assistance to the cryptanalysts, and undertaking code recovery.

d. The Japanese Commercial Translation Section, Language Branch, which works adjacent to the cryptanalytic units and is responsible for the code recovery and translation of systems which are non-diplomatic in nature. See control survey of this section.

TAB K

e. The Japanese Translation Section at Vint Hill Farms Station, which performs some decoding on systems, essentially low grade in cryptographic complexity, which have been assigned to them by the Japanese Diplomatic Section, and which further assists in compiling a Japanese dictionary.

f. The Kana Sorting Unit of General Analysis Section of Traffic Analysis and Control Branch, which is located in the same wing with the cryptanalytic and translation units, and sorts and distributes kana traffic from the Japanese communications net, which has been named the Japanese Domestic Network.

g. The Bulletin Section of the Information and Liaison Branch to whom all translations are delivered and from whom the worksheets and bulletin copies are returned.

h. The Government Code and Cipher School and the Canadian Center at Ottawa with whom a division of labor both in research and exploitation has been effected.

4. Personnel.

a. The following is a list of the number of personnel employed in the Japanese Diplomatic Section:

Male Officers	- 2
WAC Officers	- 0
Enlisted Men	- 1
Enlisted WAC	- 2
Military Personnel	- 5
Civilians	-90
Total Personnel	-95

b. In addition to this personnel, there are 61 people attached to the problem by the Language Branch.

c. The personnel of this section work on three shifts, with the majority on the day shift.

d. The personnel currently assigned to the section are inadequate to execute the total mission of the section, due to lack of trained cryptanalytic personnel. The Japanese Diplomatic Section is unable to undertake research and recovery of many Japanese Diplomatic and Commercial systems which contain intelligence of value to the prosecution of the war. This fact has in practice resulted in a modification of the mission of the section, so that the mission is currently based on what it is possible to undertake, considering the shortage of personnel, rather than on the research and exploitation of all Japanese systems.

e. It is estimated that in order to accomplish the total mission of the section the following additional personnel would be required in the sections:

	Experienced Analysts	Experienced Analytic Aides	New Analytic Aides	Total
Research Subsection	8	7	10	25
Development Subsection	-	5	5	10
Total	8	12	15	35

5. Space. The space allocated to the section is adequate and its location in respect to other units is convenient, with the exception of the fact that it is separated by three wings and one floor from the Japanese Diplomatic Translation Section, to which the decoding of every Japanese diplomatic message must be taken, and from whom all scanned and translated messages must be returned. This physical separation results in a considerable waste of time and energy between these sections. A floor plan of this section is attached as Inclosure 2.

6. The lighting of the wings is considered inadequate.

7. Files.

a. The following files are maintained in the Japanese Diplomatic Section:

(1) Administrative correspondence and records.

(2) Technical correspondence, studies, and reports. Historical material and current material used in common by the various subsections is filed in the Administrative office. Current material relevant to particular problems is filed in the appropriate subsection.

(3) Code instructions and technical cross-references - filed in the Administrative office.

(4) Technical analytic materials and worksheets. Historical materials are filed in the Administrative office or storage. Current materials are filed in the appropriate subsections.

(5) Traffic and decodes. Originals in process are handled by the appropriate subsection. When processed they are filed in the Traffic Subsection or storage. Dupes are filed in the appropriate subsection.

(6) Traffic logs and indexes. Master logs and indexes are filed in the Traffic Subsection or storage. Necessary additional logs for particular systems are maintained in the appropriate subsection.

(7) Bulletin copies. Filed in the Traffic Subsection or storage.

b. Traffic dupes are kept for 6 months. Obsolete administrative correspondence and records are destroyed every 6 months. Remainder of files are kept permanently.

c. With regard to the possibility of eliminating unnecessary files now maintained in the Japanese Diplomatic Section, it was suggested

that the file of bulletin copies be destroyed after six months, except for those bulletins dealing with code instruction. The Officer in Charge of the section agreed to this suggestion.

8. Reports.

a. The following reports are prepared by the Japanese Diplomatic Section:

(1) Weekly strength report - originated by Administrative Office and submitted to Chief, General Cryptanalytic Branch.

(2) Monthly strength report - originated by Administrative Office and submitted to Chief, General Cryptanalytic Branch.

(3) Semi-monthly Roster of Enlisted Assignments - originated by Administrative Office and submitted to Chief, General Cryptanalytic Branch.

(4) Weekly night-shift roster - originated by Administrative Office and submitted to Chief, General Cryptanalytic Branch.

(5) Weekly night-shift supervision roster - originated by Administrative Office, and submitted to Chief, General Cryptanalytic Branch.

(6) Daily technical report - originated by Administrative Office, and submitted to General Cryptanalytic Branch Recorder.

(7) Semi-monthly technical report - originated by all subsections of Japanese Diplomatic Section, and submitted to Administrative Office of this section.

(8) Semi-monthly technical report - originated by Administrative Office and submitted to General Cryptanalytic Branch Recorder.

(9) Daily systems report - originated by all subsections, and submitted to Administrative Office of Japanese Diplomatic Section.

(10) Monthly systems report - originated by Administrative Office and submitted to Control Office.

9. Organization and Work Flow.

a. The traffic which is received in the Japanese Diplomatic Section is of two principal types:

TOP SECRET

(1) Japanese Diplomatic and Greater East Asia Ministry traffic received from International Point to Point circuits, and from the Far Eastern Diplomatic Net.

(2) Japanese Commercial, Minor Governmental, and Private traffic which is received from the Japanese Domestic Net.

b. Traffic of the first type is received in the Traffic Subsection, where it is identified as to cryptographic system, indexed, logged, and distributed to the subsections concerned for further processing.

c. Traffic which is in one of the machine cipher systems is turned over immediately from the Traffic Subsection to the Machine Subsection. This subsection indexes its own traffic, solves the machine settings, and deciphers the messages on the cipher machine. The subsection is set up separately partly because it represents a unique Japanese cipher system which can be handled independently, and partly because it is believed that additional security applies to the fact of the solution of this most secure Japanese system, and for this reason it is isolated from the rest of the section.

d. Traffic which is in systems which have been completely solved is turned over to the Decode Subsection. This section is responsible for the decoding and deciphering of these systems. For reasons of convenience and for best utilization of personnel, the personnel (colored) of the Commercial Section of the General Cryptanalytic Branch perform the decoding of the system JAH. More complete description of this activity is available in the survey of the Commercial Section.

e. Traffic which is in systems which have been partially solved is turned over to the Development Subsection, where such messages as can be read are decoded or deciphered, and those which cannot be read are added to the cryptographic depth to aid in further recovery of unsolved elements of the system.

f. Traffic in systems which have not been solved is turned over to the Research Subsection for study.

g. Decodes which are made in the Machine Subsection, the Decode Subsection, and the Development Subsection, are then sent to the Japanese Diplomatic Translation Section of Language Branch, where they are scanned, and those which are of importance are translated.

h. All decodes are returned from the Japanese Diplomatic Translation Section to the Traffic Subsection of the Japanese Diplomatic Section, General Cryptanalytic Branch. Here the messages which have not been translated are filed in the Traffic Subsection. Messages which have been translated are further processed for the addition of relevant relay and cross reference

information before they are sent to the Bulletin Section of Information and Liaison Branch for publication and dissemination. This processing consists of adding such information as call signs, indicators of further routing, etc.

i. Traffic of the second type, as listed in paragraph 9 a (2) - that is, of the Japanese Domestic Net - is received in the Japanese Diplomatic Section from the Kana Sorting Unit of the General Analysis Section of the Traffic Analysis and Control Branch. This sorting unit works in the same wing as and in close proximity to the sections which process the traffic. Traffic in readable systems is turned over to a group of decoders who are a part of the General Cryptanalytic Branch. These decoders are located in the same area as the translators, and they work closely in the production of intelligence.

j. Plain text messages are handed to the translators for scanning. Those of immediate operational use are translated on the spot; those which are obviously unimportant are destroyed; and the relative importance of the rest of the messages is indicated and they are then sent to the Japanese Nisei Unit at Vint Hill Farms Station for translation.

k. Traffic in systems which are under study is turned over to the Research Subsection of the Japanese Diplomatic Section.

l. The work flow of this Domestic Net traffic is very well under control. This is obviously due to the complete integration of the work of the units of General Cryptanalytic Branch, the Traffic Analysis and Control Branch, and the Language Branch. The physical location of all of the units in one area and the spirit of cooperation between them has greatly contributed to their effectiveness.

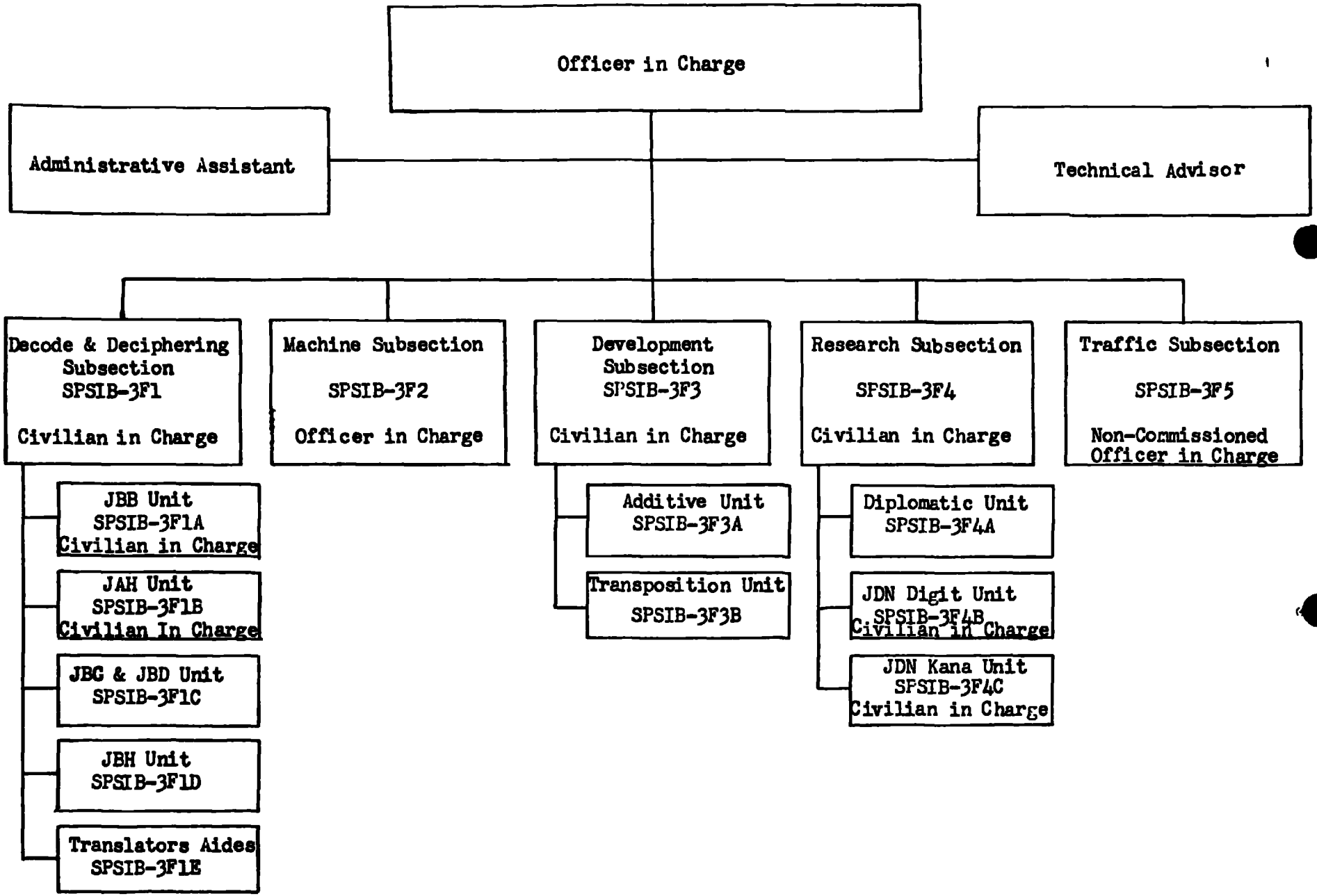
2 Incls
1. Org Chart - SPSIB-3F
2. Floor Plan - SPSIB-3F

TOP SECRET

REF ID:A70871

~~SECRET~~

JAPANESE DIPLOMATIC SECTION, SPSIB-3F



~~SECRET~~

REF ID:A70871

JAPANESE
COMMERCIAL SECTION

LANGUAGE BRANCH

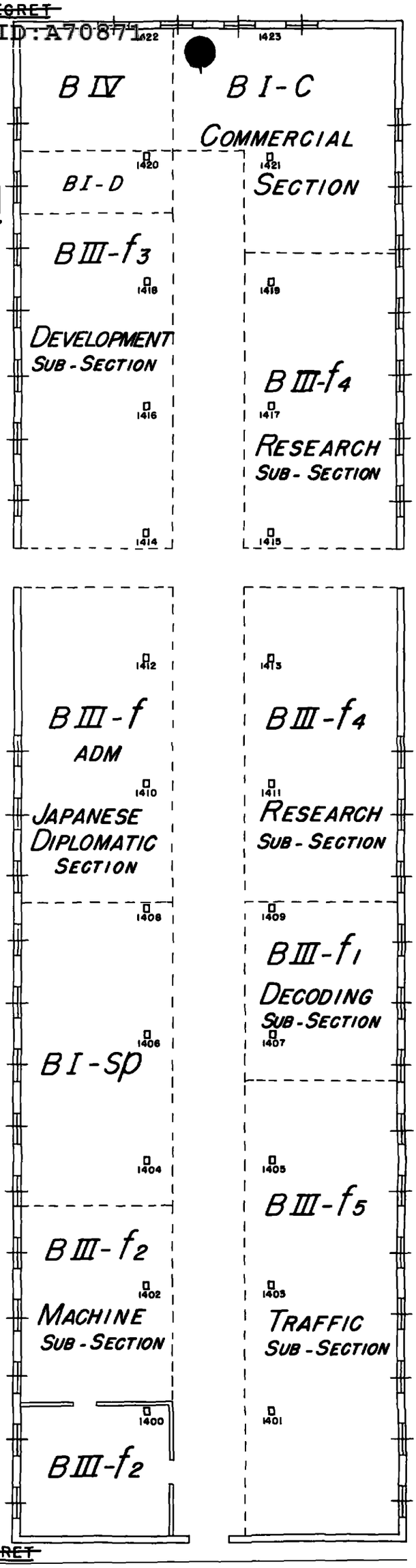
SPSIB - IC

WING 4
1ST FLOOR
OPERATIONS "B"

JAPANESE
DIPLOMATIC SECTION

GENERAL CRYPTANALYTIC BRANCH

SPSIB - III f



SPSIB-1A

REF ID:A70871

JAPANESE COMMERCIAL TRANSLATION SECTION, SPSIB-1C
LANGUAGE BRANCH, SPSIB-1

1. The mission of the Japanese Commercial Translation Section is the bookbreaking and translation of all Japanese language commercial messages - that is, non-army and non-diplomatic traffic - which are intercepted on the Japanese Domestic Net. This section also supplies G-2 with specific information concerning locations of industrial establishments, production figures, railroad lines and bridges, etc., for use in the strategic bombing and submarine campaigns and in the economic studies being made of Japan's ability to wage war. In addition, a scanning group in this section has the mission of clarifying inferences from plain text in volume which might yield material of intelligence value, and scanning all plain text messages in order to designate the messages that are to be translated by the Translation Unit at Vint Hill.

2. Because of the small number of people employed in this section, it is not broken down into subsections, and therefore an organizational chart is not included.

3. The Japanese Commercial Translation Section is closely integrated with the following units:

a. Kana Sorting Unit of Traffic Analysis and Control Branch.

b. Shipping Section of Information and Liaison Branch.

c. Japanese Diplomatic Section of General Cryptanalytic Branch.

4. Personnel.

a. The following is a list of the personnel assigned to the Japanese Commercial Translation Section:

Male Officers	- 3
WAC Officers	- 2
Enlisted Men	- 8
Enlisted WAC	- 0
Military Personnel	- 13
Civilians	- 6
Total Personnel	- 19

TAB L

TOP SECRET

b. The foregoing personnel is adequate to perform the mission assigned to the section.

5. Space.

a. The Japanese Commercial Translation Section is located in the rear of Wing 4, first floor, Operations "B". The space assigned to this section is adequate. (A floor plan of this section is included with the floor plan of the Japanese Diplomatic Section, General Cryptanalytic Branch in Tab K.

b. The location of this section is convenient for contact with other sections, particularly the Kana Sorting Unit of Traffic Analysis and Control Branch, and the Japanese Diplomatic Section of General Cryptanalytic Branch.

6. The lighting in this section is adequate, as the section is located in the rear of the wing.

7. Files.

a. The following files are maintained in the Japanese Commercial Translation Section:

(1) File of company names and cable addresses appearing on the Japanese Domestic Net.

(2) Three-way traffic file, by date, worksheet number, and H-number.

(3) Solution file of the systems being exploited or which have been exploited.

b. The length of time that the files are maintained varies from three months for dead-headed systems or parts of systems, to indefinitely for unsolved material.

8. Reports. The following reports are rendered by the Japanese Commercial Translation Section:

a. Trigraph reports which are prepared monthly and submitted to the Control Office.

b. Semi-monthly progress report submitted to the Chief, Language Branch.

9. The reference material utilized by this section consists of information obtained from the Special Projects Section of Language Branch, the Information Section of Information and Liaison Branch, and the Economic Branch of G-2. Because of the present size of the section, it is not necessary to maintain a central system of reference material, although if and when the section increases, it may be necessary to establish a definite file of reference material.

10. A more complete description of the work flow of this section is to be found in the work flow of the Japanese Diplomatic Section of the General Cryptanalytic Branch, Tab K.

JAPANESE DIPLOMATIC TRANSLATION SECTION, SPSIB-1D
LANGUAGE BRANCH, SPSIB-1

1. The mission of the Japanese Diplomatic Translation Section is the translation of Japanese Diplomatic traffic, and the assisting of the General Cryptanalytic Branch cryptanalysts with code instruction messages.

2. The Japanese Diplomatic Translation Section is composed of four subsections, as illustrated on the organizational chart attached as Inclosure 1.

3. The Japanese Diplomatic Translation Section works in close liaison with the following units:

a. Japanese Diplomatic Section of General Cryptanalytic Branch.

b. Information Section of Information and Liaison Branch.

c. Bulletin Section of Information and Liaison Branch.

More details of the integration of this section with cryptanalysis will be found in control survey of Japanese Diplomatic Section of General Cryptanalytic Branch.

4. Personnel.

a. The following is a list of the personnel employed in the Japanese Diplomatic Translation Section:

Male Officers	- 7
WAC Officers	- 0
Enlisted Men	- 20
Enlisted WAC	- 0
Military Personnel	- 27
Civilians	- 15
Total Personnel	- 42

TAB M

b. The personnel in this section is adequate to perform the mission assigned.

5. The Japanese Diplomatic Translation Section is located in the headhouse, at the head of Wing 1, second floor, Operations "B". A floor plan of this section is attached as Inclosure 2. Although the space allotted seems adequate, there is some question as to the convenience of the location of this unit in respect to the other units with which it works most closely. The factors which militate in favor of moving the section are:

a. All Japanese Diplomatic messages which are decoded must be carried from the fourth wing, first floor to the headhouse of the first wing, second floor, for scanning and translating, and must then be returned.

b. The other sections with which the translators have closest operational contact (Information and Bulletin Sections of Information and Liaison Branch) are all located in the fifth wing, first floor.

6. The factors which militate against moving the section are:

a. The translators prefer the peace and quiet of the headhouse.

b. The location is convenient to the Administrative Office of the Language Branch.

7. The lighting in this section is adequate.

8. Files.

a. The following files are maintained in this section:

(1) Current H, T, C.I. and SJE series of Japanese diplomatic messages - maintained for 6 months.

(2) British cabled translations of Japanese diplomatic messages - kept permanently.

(3) Magic Diplomatic Summaries back to 5 February 1945 - kept permanently.

(4) Reference file containing materials for daily use by this section - kept permanently.

9. The following reports are rendered by the Japanese Diplomatic Translation Section:

a. Semi-monthly reports - submitted to the Chief, Language Branch.

b. Periodic efficiency reports.

10. The following is a list of the reference material used by this section:

a. Lists of Japanese personnel.

b. Lists of Chinese personnel.

c. Railroad studies from the Information and Liaison Branch.

TOP SECRET

d. Magic Diplomatic Summaries.

e. Dictionaries.

f. Ship lists.

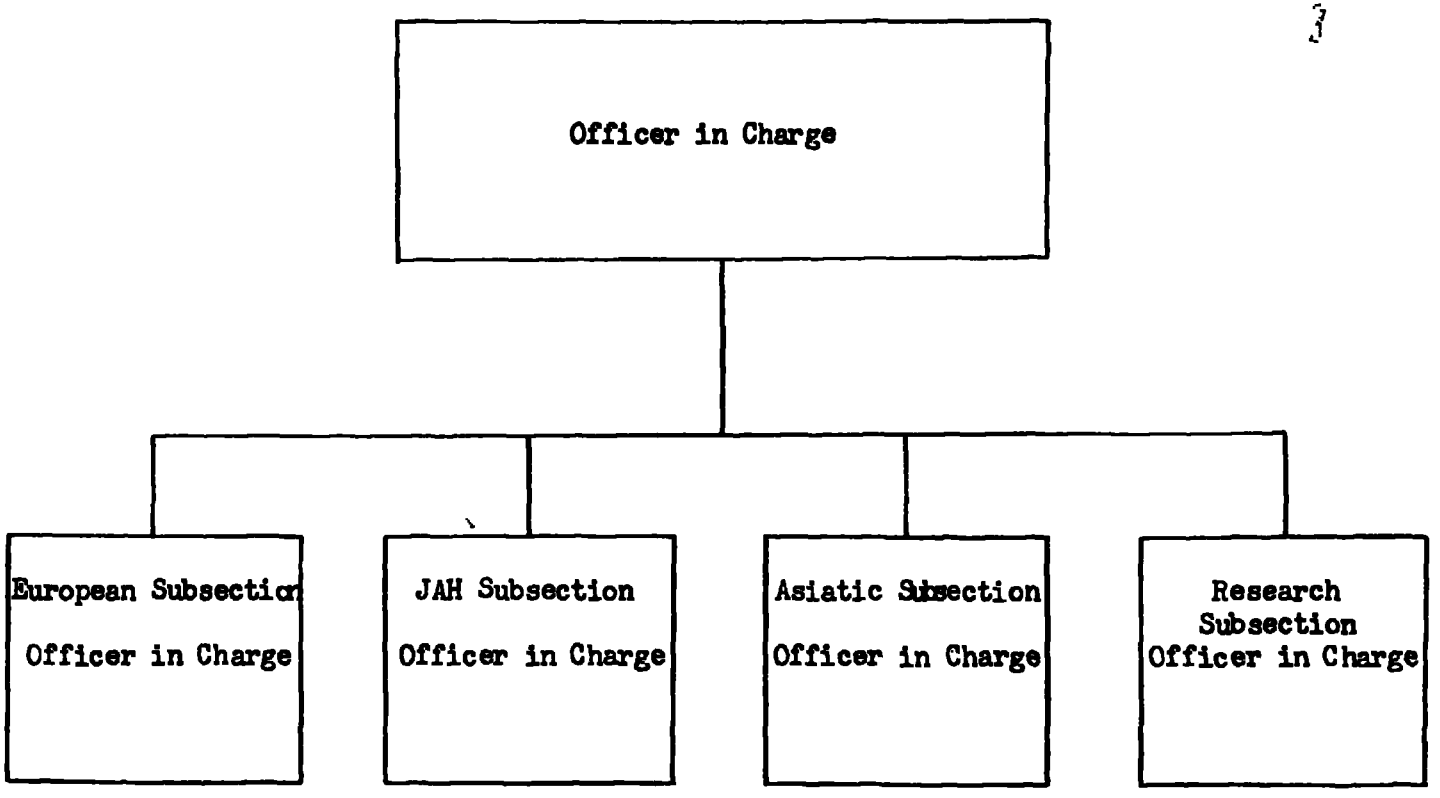
g. Reports on iron, alumina, etc., in China and Manchukuo.

2 Incls
1. Org Chart SPSIB-1D
2. Floor Plan SPSIB-1D

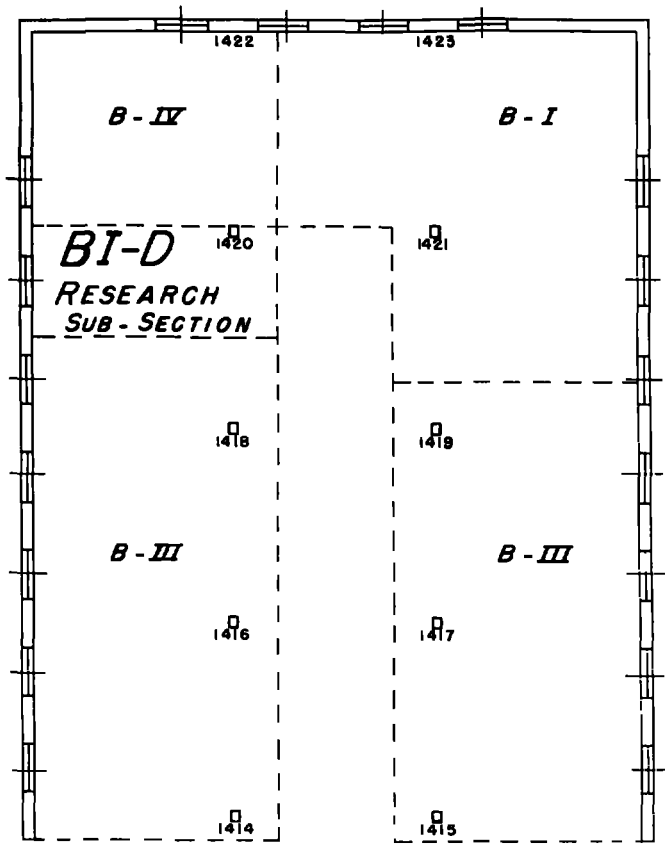
TOP SECRET

~~SECRET~~

JAPANESE DIPLOMATIC TRANSLATION SECTION, SPSIB-1D



REF ID:A70871



1ST FLOOR

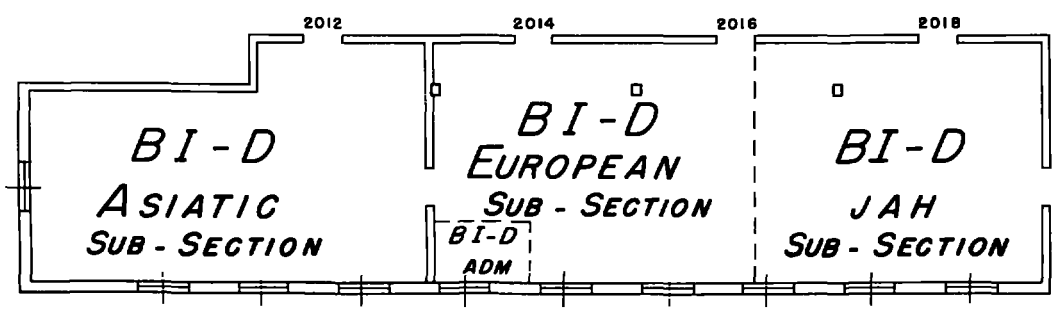
BACK OF WING 4

JAPANESE DIPLOMATIC TRANSLATION SECTION

LANGUAGE BRANCH

SPSIB-ID

OPERATIONS "B"



2ND FLOOR

HEAD HOUSE - OPPOSITE WING 1

SPECIAL PROBLEMS SECTION, SPSIB-30
GENERAL CRYPTANALYTIC BRANCH, SPSIB-3

1. The mission of the Special Problems Section is to discover as much information about Russian traffic as is possible.

2. Organization.

a. The organization of the Special Problems Section is unique in that each person reports directly to the section chief, rather than the section being divided into subsections and units. The organizational chart, attached as Inclosure 1, indicates that the functions on a staff level are divided into 8 categories, and that the cryptanalysts are placed on teams that work together, but who are directly responsible to the Officer in Charge of the Special Problems Section. The advantage of this type of organization is that the cryptanalysts, translators, and personnel engaged in the exploitation of Russian traffic are not concerned with the administrative details of their subsection or unit, and therefore, they can devote their entire time to their own specific problem.

b. Because of the highly classified nature of the work in this section, there are several additional duties performed by the Special Problems Section which are not performed by any of the other sections of the General Cryptanalytic Branch.

(1) It is the duty of this section to type up the daily bulletin of the messages translated, rather than the Bulletin Section of the Information and Liaison Branch. Copies of these messages are handcarried to the Deputy Chief of Staff, Military Intelligence Service.

(2) A file of collateral information is maintained in this section, which would ordinarily be kept in the Information Section of Information and Liaison Branch.

3. There is no liaison maintained between this section and any other section or unit of the Signal Security Agency, except the General Cryptanalytic Branch Administration Office. The Special Problems Section does maintain contact with the section at the Naval Communications Annex engaged in the study of Russian problems.

4. Personnel.

a. The following is a list of the personnel employed in this section: TAB M

Male Officers - 5
Civilians - 94

Total Personnel - 99

b. At least 100% expansion in personnel will be required in this section. However, it is believed that an increase of 20% of the personnel each month would provide for necessary expansion and still would not endanger security.

c. Personnel for this section usually are recruited from small towns, and from persons who have a religious background. People who are graduates of large universities and who majored in economics are not accepted, without further check on their loyalty.

d. In selecting the personnel from the Civilian Training School, they are questioned as to their likelihood of remaining more or less permanently on the job. This is done in the interests of security, and continuity of the work flow.

5. The Special Problems Section is located in the sixth wing, second floor, Operations "A", separated from an adjoining section only by movable partitions. This location is not satisfactory for maintenance of security. Because of the distance between this section and the Administration Office of the General Cryptanalytic Branch, the location is not convenient. It is believed that this section should occupy the whole wing, or a closed room in some other location.

6. The lighting in the Special Problems Section is completely inadequate.

7. Files.

a. The following files are maintained in this section:

(1) Administration correspondence and records.

(2) Collateral information files.

(3) Cryptographic collateral file.

(4) Technical inventory.

(5) Traffic.

b. These files are all maintained indefinitely, except for the administration files, which are placed in an obsolete file at the end of the year.

8. The following reports are rendered by the Special Problems Section:

a. Monthly man-hour report submitted to the General Cryptanalytic Branch.

b. Semi-weekly technical report submitted to the General Cryptanalytic Branch.

c. Occasional technical reports on solutions submitted by cryptanalysts, distributed internally, and in a few cases, to the Navy.

d. Systems reports submitted to the General Cryptanalytic Branch.

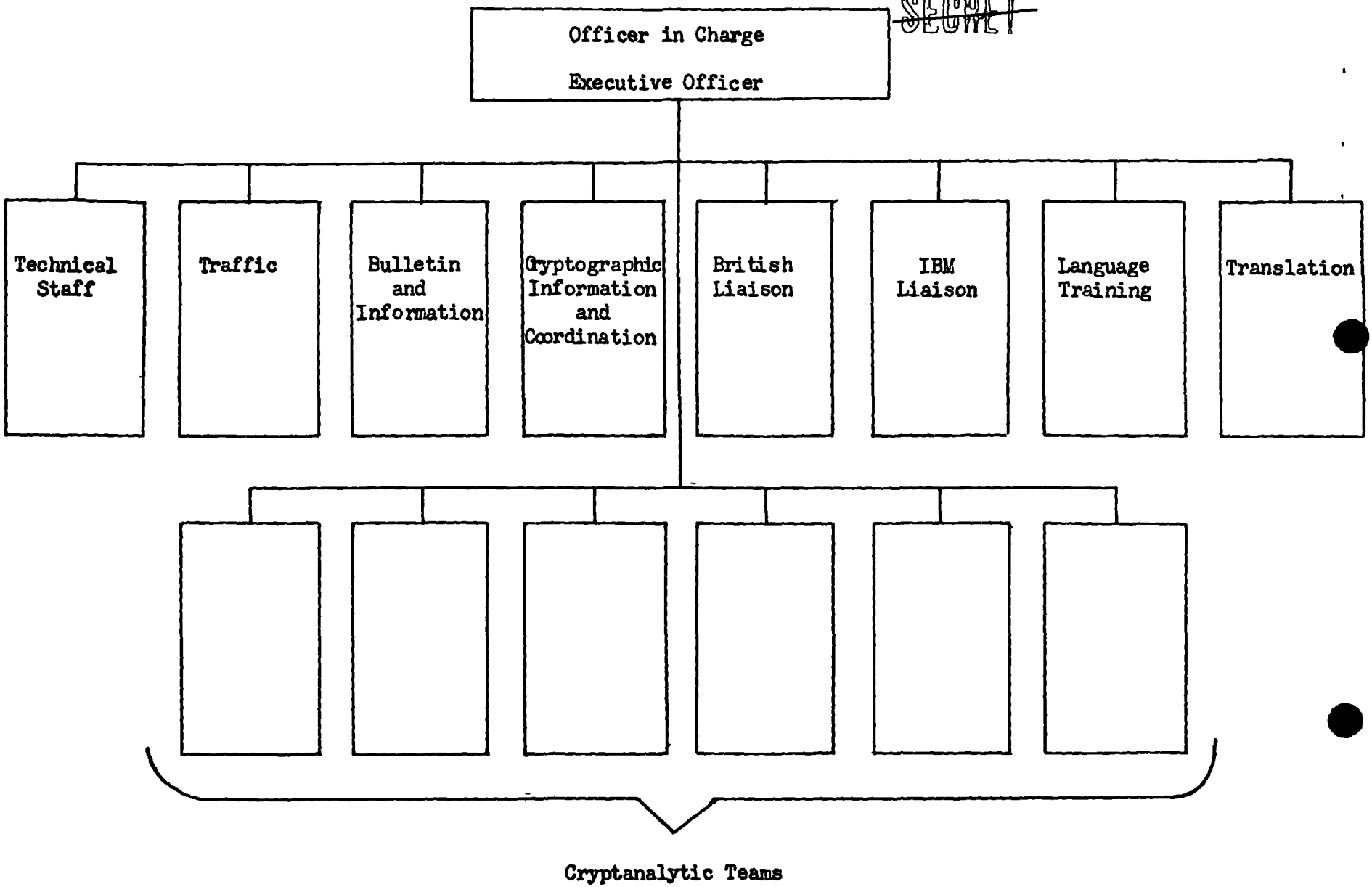
e. Miscellaneous personnel reports.

1 Incl
Org Chart - SPSIB-36

REF ID:A70871

SPECIAL PROBLEMS SECTION, SPSIB-3G

~~SECRET~~



~~SECRET~~

INFORMATION SECTION, SPSIR-6
INFORMATION AND LIAISON BRANCH, SPSIR

1. The mission of the Information Section of Information and Liaison Branch is as follows:

a. To receive, record and to distribute throughout Signal Security Agency classified documents and similar materials of value to the operating units.

b. To supply operational, background and documentary information to cryptanalysts and translators.

c. In cooperation with the Who's Who Branch of the Military Intelligence Service to effect an exchange of processed information which enables each to have available more wanted information than either could provide alone.

d. To provide an index of information (exclusive of that relating to certain economic topics) appearing in the Signal Security Agency Bulletin.

e. To acquire, catalog, distribute, care for unclassified books and other reference materials of value to the Signal Security Agency.

2. The Information Section is divided into three main subsections, plus the Signal Security Agency Library, as illustrated on the organizational chart attached as Inclosure 1.

3. This section works in close liaison with the following units:

a. All branches of the Intelligence Division for information helpful in cryptanalysis and translation.

b. All operating units of the Signal Security Agency as occasion arises for them to obtain books, classified documents or information on special topics.

4. The following is a list of the personnel employed in the Information Section:

Male Officers	- 2
WAC Officers	- 0
Enlisted Men	- 1
Enlisted WAC	- 3
Military Personnel	- 6
Civilians	-71
Total Personnel	- 77

TAB
0

b. The aforementioned personnel work on the day and swing shifts.

c. This personnel is not adequate to perform the mission assigned to the section, but the necessary requirements have been requisitioned. The greatest difficulty of the section has been to secure employees with the right combination of interest, intelligence and alertness, and individuals who are mentally keen, adaptable and capable of exercising considerable independent discretion in the processing of the work assigned to them.

5. Space.

a. The Information Section is located in the fifth wing, the headhouse opposite the fifth wing, and the headhouse opposite the sixth wing, first floor, Operations "B". A floor plan of this section is attached as Inclosure 2.

b. The space in this section is not adequate to completely house all of the file cabinets necessary.

c. This location of the Information Section is not convenient for contact with other sections, as, for instance, the sections of the General Cryptanalytic Branch, located in Operations "A".

6. The lighting in this section is adequate.

7. Files.

a. The following files are maintained in the Information Section:

(1) Biographical Unit.

(a) Master File - Contains one card for each name entered in the other files of the unit, and serves as key to where more detailed information is available.

(b) Country Files - Contain information about all personalities from all sources available to the Information Section.

(c) Special Files - Contain information on diplomats and their activities, government officials and their activities, non-Japanese ships and military affairs, science and technology.

(2) Geographical Unit.

(a) Master File - Contains one card for each geographical name entered in the other files of the unit, and serves as key to where more detailed information is available.

(b) Country (or Area) Files. Contain information on all geographical places, derived from all sources available to the Information Section.

(c) Special Files. Contain gazetteers, maps and handbooks; Japanized versions of place names with (so far as practicable) Chinese characters; files of POW camps, airfields.

(3) Topical Index. All H, D, L, T, CI messages filed according to the topics with which they deal, except such messages as are handled by specialized units at Signal Security Agency or the Pentagon.

(4) Point-to-Point. All H, D, L, T, and CI messages filed alphabetically according to point of origin and destination, and under this, by message number within the year.

b. Processed information and significant documents, books and similar reference materials are kept permanently. None of the files have been labelled obsolete because of the service this section performs for other units.

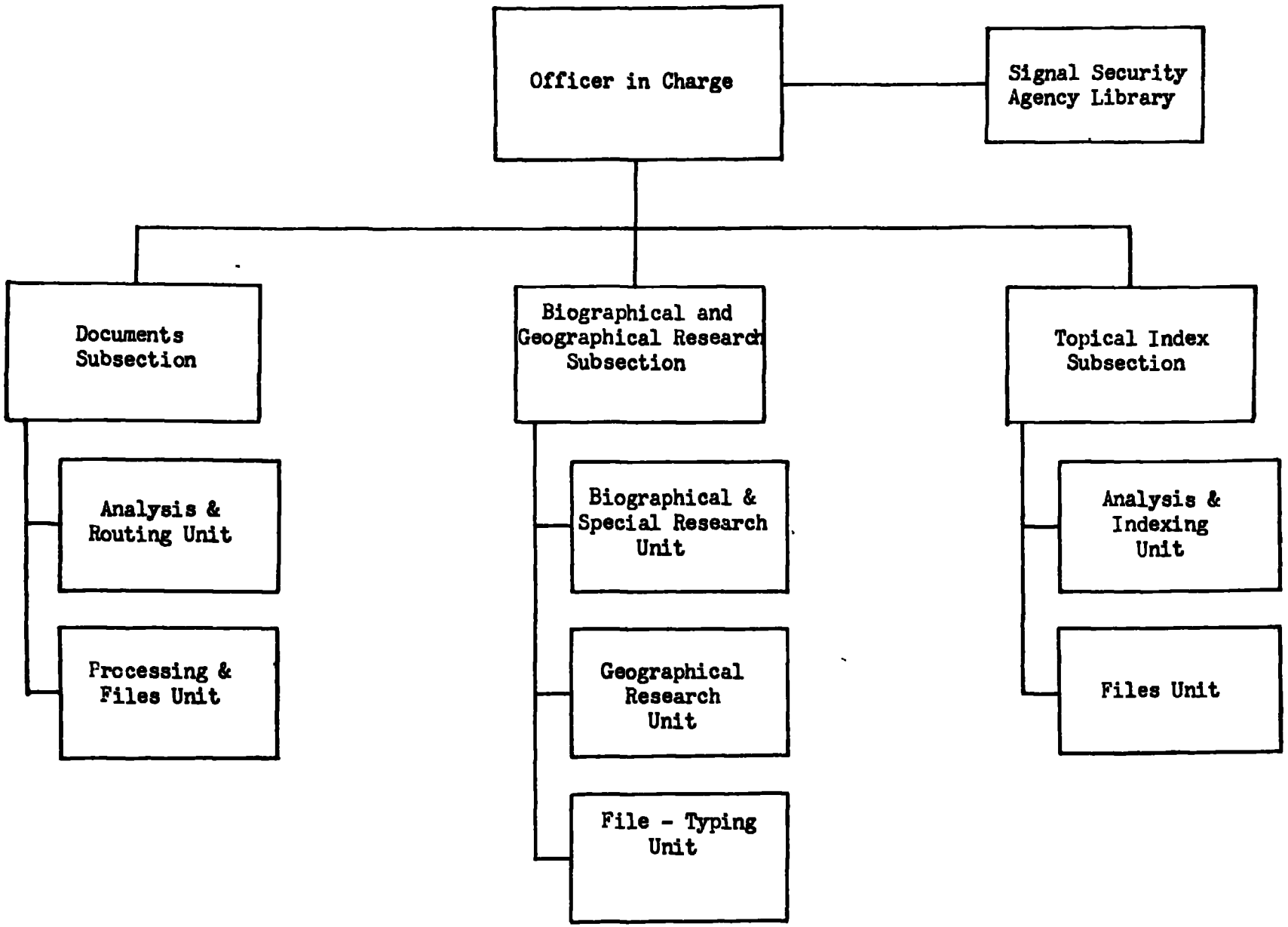
8. The following reports are rendered by the Information Section:

a. Who's Who in Diplomacy - monthly supplement distributed in the Signal Security Agency and outside.

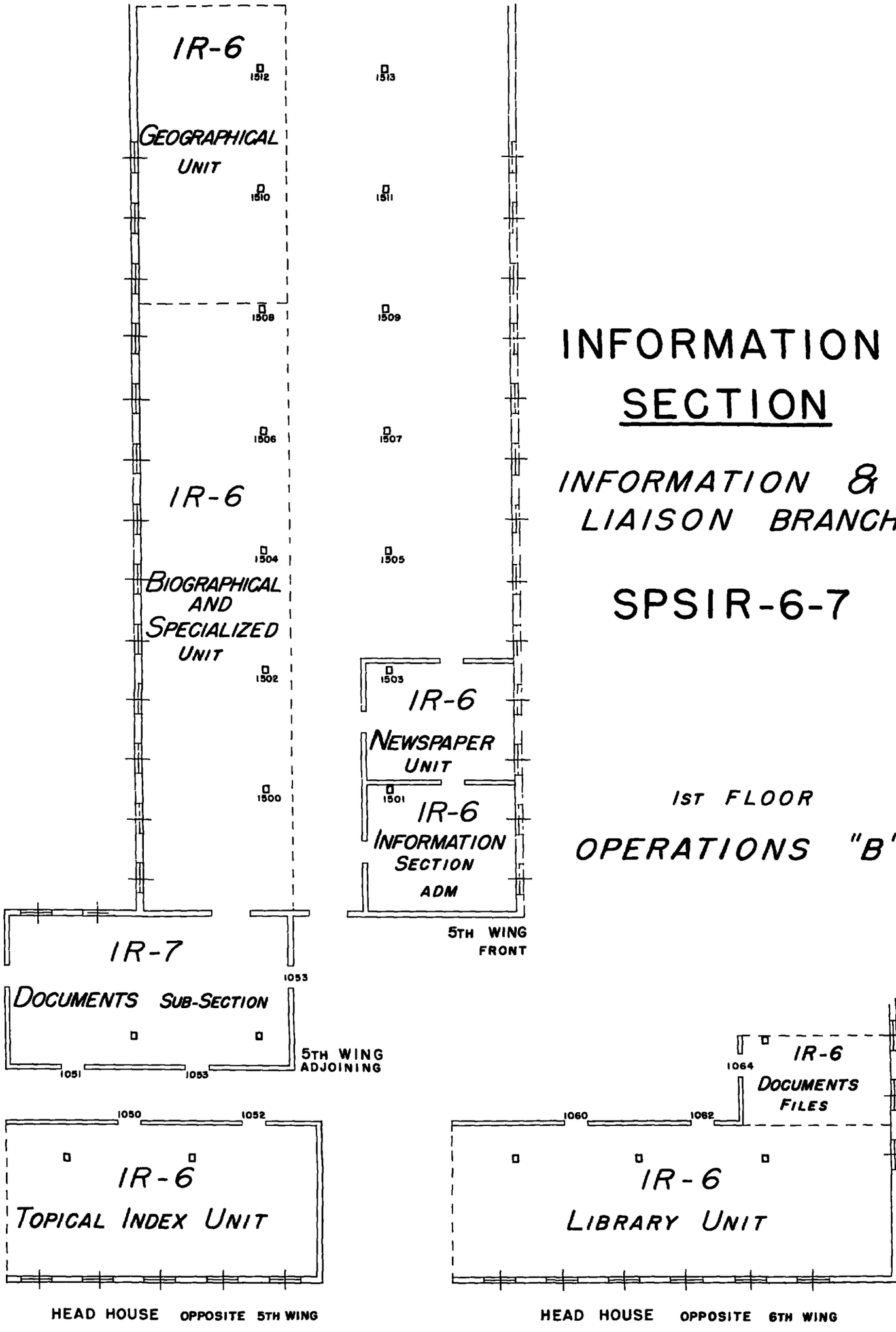
b. Special reports, as required.

c. Reports compiled from materials on file, which remain in the file for reference and additions.

2 Incls
1. Org Chart - SPSIR-6
2. Floor Plan - SPSIR-6


Officer in Charge
Signal Security Agency Library
Documents Subsection
Analysis & Routing Unit
Processing & Files Unit
Biographical and Geographical Research Subsection
Biographical & Special Research Unit
Geographical Research Unit
File - Typing Unit
Topical Index Subsection
Analysis & Indexing Unit
Files Unit

REF ID:A70871



INFORMATION SECTION

INFORMATION & LIAISON BRANCH

SPSIR-6-7

1ST FLOOR

OPERATIONS "B"

PROPOSED PRIORITIES CONTROL UNIT

1. As set forth in paragraph 11 of the overall report of the General Cryptanalytic Problem, there is an evident need for more control in the establishing of priorities concurrent with an adequate review of the product of intercept. As stated, there are really two problems to be faced which are interdependent and are best solved by considering them in relation to each other.

2. The first of these problems is the setting of priorities in all fields of the work of the General Cryptanalytic Problem. The major items to be considered here are intercept priorities for desired intelligence research priorities, exploitation priorities, and translation priorities. Intercept priorities for intelligence, research and exploitation priorities are dependent on two factors - naturally, the intelligence requirements, and secondly, the technical requirements of cryptanalysis. Translation priorities, however, are dependent almost entirely upon intelligence requirements.

3. In establishing priorities for these activities there must be established a method whereby the work produced and the energy expended in the process of meeting priority standards are consistently and constantly reviewed, in order to determine:

a. Whether the priority is actually being followed.

b. What the priority is actually accomplishing in time, personnel, facilities, and the relative importance of this expenditure.

4. There is set forth in the following an outline of a section, of a staff, to accomplish these objectives. This outline is based upon the following considerations:

a. That the Military Intelligence Service, while in a position to give general directives as to intelligence requirements, cannot give spot priorities requiring sudden changes in intercept missions, relative value of two specific messages before they are translated, or any other type of detailed direction.

b. That it is necessary to have as much detailed direction as possible, within the limits of efficient operation.

c. That the Signal Security Agency is actually an intelligence evaluation organization in that it performs a continuous process of evaluation each time a message is read but not translated.

d. That the Military Intelligence Service will not immediately be reoriented to a degree sufficient to allow it to give detailed intelligence direction to the Signal Security Agency.

e. That it is possible, with the sources of collateral information available, to establish at least minimum intelligence standards which may be applied to priorities.

f. That the more complex problem in establishing priorities is the balancing of technical requirements plus determination of what constitutes important intelligence.

g. That most of the elements necessary for priority control exist within the Agency and need only to be coordinated.

4. There are two functions which are currently being performed by the Trends Research Unit which would form an integral part of a priorities unit. These are: Subject Matter Category Studies, and the Rating of the Intelligence Value of Messages.

a. Subject Matter Category Studies. These are studies made of messages being published with a view to determining the types of information carried in each cryptographic system read at the Signal Security Agency. This function should be assigned to the priorities unit and operate in the following manner:

(1) When a new system becomes readable, a good sample of messages from all circuits should be translated or summarized and studied. Subject matter categories of the information transmitted in the systems should then be set up.

(2) No more studies should then be made until some change, such as the introduction of a new system or the discontinuance of an old system upsets the cryptographic communications balance of the country concerned - or 3 months later, whichever of these events occur first.

(3) These categories, combined with a cryptographic evaluation of the system, should be used to determine the relative position of the system in the scheme of communications of the foreign government.

b. Rating of the Intelligence Value of Messages. This function of the Trends Research Unit should be attached to the priorities unit, to operate as follows:

(1) Read all published messages.

(2) Rate these messages according to any agreed-on scale on the basis of information obtainable from the current information specialists who would also be attached to this unit.

(3) Set up an automatic procedure for a review, on a monthly basis, of the value of messages in each producing system

compared to the time lag of messages of most importance to determine if there is any place when additional personnel or procedures may be required to speed up the processing of a system with a high volume of high value messages.

6. Another function which is in existence within the Intelligence Division and which could be easily oriented to the problem of priorities is the Current Situation Room. The personnel of this unit have been trained to analyze political and economic events. The application of their work to the problem at hand would entail operation along the following lines:

a. The analysts would read newspapers such as the New York Times; they would also read the total bulletin, and the State Department cables.

c. The process of reading these items will keep the personnel well informed on current affairs.

d. The crucial point of their duties, however, would be the critical examination of State Department cables. Signal Security Agency receives copies of briefs of all cables going to or from the State Department. From a critical reading of these cables it is possible to determine in large measure and in good detail the subjects on which the State Department lacks information. It would then be the duty of this unit to inform the heads of production sections that messages dealing with these subjects should be translated, the geographical location of points where messages of desired intelligence would probably pass, and to give some explanation of their importance. A further refinement of this function would be the calling to the attention of the heads of the production sections the fact that the particular subject matter is usually transmitted in a particular system or systems (which information would be available from the subject matter category records). Another application of the work of this unit would be the noting of subjects which are items of comment and reports by the representatives of numerous countries in a particular world capital. A spot check of the countries in whose readable systems the subject did not appear, but might reasonably be expected to appear, might lead to the assumption of a crib for immediate or future application to a system of that country which was under study. These are patterns of the methods in which the Current Situation Room activities could be brought to bear directly on operations.

7. Added to these functions would be the technical activities of the Planning and Priorities Office of the General Cryptanalytic Branch, performing the same duties as at present.

8. Also, a member of the intercept control group would be a member of this priority staff group.

9. It is believed that if a priorities unit were set up along the lines indicated in the foregoing, and the details of operation worked out in common by personnel who have been performing the separate functions, a great advantage would result in the control of the activities concerned with the General Cryptanalytic Problem.