ARMY SERVICE FORCES
SIGNAL SECURITY AGENCY
WASHINGTON 25, D. C.

SPSIC

19 January 1945

MEMORANDUM for Chief, Security Division

Subject: Comments on SPSIS-3 Memorandum, dated 6 January 1945, inclosed

1. The problem, as presented by the paper, is one of placing responsibility to insure that suitable action is taken when compromises occur. In the case of systems over which Signal Security Agency exercises control, the responsibility has already been fixed upon the Security Division. The responsibility for taking action in cases where the system is not under Signal Security Agency control appears to lie with G-2, but Signal Security Agency can do no more than recommend to G-2 that they assume such responsibility.

a. The Chief, Security Division, is presently charged with the responsibility for providing adequate security for all U. S. Army signal communications. Taking proper action in cases of cryptographic compromises is one sub-phase of this responsibility. Where the cryptographic compromise involves a War Department System, direct action can be and is taken.

b. Paragraphs 1 and 3 of the RECOMMENDATIONS of the subject paper are therefore redundant and there exists no plausible reason why paragraph 6a of the RECOMMENDATIONS is not the one and only one solution as to the location for this responsibility.

c. Paragraph 6b and 6c of the RECOMMENDATIONS have no bearing on the problem of responsibility.

2. Paragraphs 4 and 5 simply state that where compromise of other than a War Department system is involved ~~[illegible]~~ the responsibility for action lies with G-2.

3. Paragraphs 2, 4, 5, 6, 7, and 8 of the discussion simply indicate that there has not been a free and well-established inter-exchange of information between G-2, Joint Security Control, Intelligence Division and the Security Division.

a. Paragraphs 2, 4, 5, 7, 8, 9, 10, 11, 12, and 13 of the recommendations simply attempt to establish liaison channels for this free exchange of information between the above mentioned agencies. With Security Division as the focal point, liaison channels to "A" Branch, another one to Intelligence Division, another to the Navy and another to G-2 should accomplish the desired result.

4. Exception is taken to paragraph 13 of the RECOMMENDATIONS, in that there does not appear to be any necessity to furnish G-2 with copies of all action radios initiated by Security Division which pertain to cryptographic compromise of systems over which Security Division exercises direct control.

5. The real purpose of the paper seems to be to point out that Security Division has not been receiving all of the information that it should have at its disposal. In the past, the control of information given to Security Division has been exercised by Headquarters, Signal Security Agency. If Security Division is given the authority to obtain the information it desires, it can immediately establish the necessary liaison channels.

6. It should be noted that the problem of evaluating Intelligence information, as it relates to communication security compromises, represents not more than 5% of the total security problem which confronts the Security Section of Security Division. While it is recognized that information from such sources is important, it must be emphasized that it should not be given a standing or importance out of proportion to that attached to the other phases of security since the information itself is valueless unless it is complemented by concurrent studies upon the other phases of security.

7. Paragraph 2 of the RECOMMENDATIONS is an accomplished fact and should not therefore be a recommendation but could probably be included in the DISCUSSION. The same could be said of paragraphs 1 and 3 of the RECOMMENDATIONS.

8. Paragraph 11 of the RECOMMENDATIONS relates to an item under the jurisdiction of Joint Security Control. G-2 itself does not at the present time have access to this information except in the person of General Bissell. Paragraph 11 should state the method by which this information should be made known to the evaluating unit.

9. Recommend following one-page staff study be substituted for SPSIS-3 Memorandum, dated 6 January 1945 and the Memorandum be attached as an appendix thereto:

PROBLEM:

1. Who is responsible for taking action on cryptographic compromises and what do they need to do the job in addition to what they have now?

FACTS BEARING ON PROBLEM:

2. Security Division of SSA is responsible for action on cryptographic compromises affecting War Department controlled systems.

3. There is no apparent fixation of responsibility for action on compromises of systems not controlled by War Department. The War Department does not, at present, exercise direct control over some Army systems.

4. Security Division has not had access to all the information required to assure doing a 100% job of paragraph 2 above.

CONCLUSIONS:

5. Security Division should have access to all information bearing on the problem.

6. The War Department should control all systems used by the Army.

7. G-2 should take action on cryptographic compromises affecting non-War Department systems.

RECOMMENDATIONS:

8. Authorize Security Division to establish necessary liaison channels.

9. Action be initiated to effect War Department control of all systems used by the Army.

10. Request G-2 to assume conclusion 7.

11. Headquarters, SSA, provide Security Division with assistance in establishing liaison, if necessary.

K. Kuhn
Lt. Col., Signal Corps

1 Incl.
SPSIS-3 Memorandum,
dated 6 January 1945

SECRET CONFIDENTIAL RESTRICTED

TO DATE 8 Jan 45 FROM

Commanding Officer
Assistant Commandant
Dir of Comm Research
Control O
Fiscal O
Administrative O
Post Adjutant
Intelligence O
Provost Marshal
2nd Sig Serv Bn
Chief, Pers & Tng Div
Chief, Pers Br
Chief, Tng Br
O/C Officer Pers Sec
Chief, Oper Serv Div
Chief, Communications Br
Chief, Laboratory Br
Chief, Machine Br
Chief, Supply Br
O/C, SSA Mail Unit
Chief, Security Div ✓
Chief, Protective Sec Br
✓ Chief, Cryptographic Br
Chief, Development Br
Chief, Intelligence Div
Chief, Language Br
Chief, Mil Cryptanalytic Br
Chief, Gen Cryptanalytic Br
Chief, T/A and Control Br
Chief, I & L Br

As discussed
As requested
Detailed Comments and return
Information and file
Information and forwarding
Information and return
Recommendation
See note on reverse
Signature if approved
Your action

SIS SC Form No. 96 (Rev)
16 Nov 44

DRAFT

SPSIS-3

6 January 1945

MEMORANDUM for

The Problem: The necessity for placing responsibility in regard to communication security compromises indicated by ULTRA information in order to insure that suitable action is taken.

I. DISCUSSION.

1. The necessity for definitely placing responsibility for action in cases of compromises indicated by ULTRA information, in order to insure that suitable corrective measures are taken, is deemed of utmost importance.

2. The Signal Security Agency can and does issue necessary instructions for placing reserve systems into effect in the case of definite compromise of United States Army codes or ciphers. This responsibility is assigned to the Cryptographic Branch. In most cases the compromise is a physical one and is reported by our own field units. In the case of a cryptographic compromise, the only means of ascertaining this fact is by observing obvious reactions of the enemy or in reading enemy code or cipher messages. The C Series of the Bulletin was set up in an attempt to segregate this type of information and route it to the Cryptographic Branch for necessary action. This method presupposes that the personnel engaged in scanning and translating can recognize this type of message and place it in the proper category. This recognition of compromises may not always be apparent even to a seasoned translator because of the separation of Japanese message in parts, some of which become readable at widely separated periods. This method further presupposes that there are personnel in the Cryptographic Branch who

can understand and evaluate the material in order that proper action may be taken. The use of Kana and other obscure terminology should therefore be either rigidly excluded from C Series messages, or explained in each message where such cases are encountered. Aside from the C classification which is made by the translator, there are other methods of screening this material. The Bulletin Section has scanners who place messages in various categories for which it makes a separate distribution. Messages which appear of interest to C and A Branches are routed to them. As in the case of the translator, the proper selection is not always apparent.

3. The Signal Security Agency can only act on compromises pertaining to systems over which it has direct control. How is proper action taken in regard to compromises of low-grade codes or ciphers prepared locally in theaters by Army Ground Forces or Army Air Forces?

4. If an intercepted message quotes United States information but does not clearly state whether the information was secured by cryptanalysis or by the reading of plain text, how is it classified according to Series, and if it is put in the C Series what action is taken by Cryptographic Branch? (See C-923 A,G). If it is not placed in the C Series, Cryptographic Branch would not necessarily see it, although attempts are made to screen this material for them in I&L Branch. Does G-2 assume the responsibility for notifying the interested commands? Of late, G-2 has been taking the initiative on some of these items (See FES #254). For instance, take F-37240-E which quotes a message from Stilwell to Chiang Kai Shek and which is labeled "A" intelligence. A G-2 report (FES #214) stated that these were Chinese code messages, but how would Cryptographic Branch know this since it does not receive copies of the Magic Summary? There have been specific

indications that the term "A" intelligence in the Japanese Army applies to that obtained from the solution or reading of code messages. This information appeared in the F Series (F-29577). Message F-38347D quotes as "A" intelligence the movements of some Allied regiments in Burma. It is not stated whether the movements were made by United States or British units. Where is the responsibility placed in order to ascertain the missing information in this case? There are also Navy ULTRA sources which occasionally show some type of compromise.

5. There are countless messages in the Bulletin which reveal Japanese traffic analysis results. Some of these are put in the C Series, which means they get to the Cryptographic Branch, but A Branch is primarily interested in this information and should have it for evaluation in order to study deception results in various theaters. Here again the Bulletin Section screens out this material for A Branch. This is not a problem involving cryptographic security, but it does involve communication security which is both a C and an A Branch concern at present.

6. There is the case of compromises of State Department systems. It is understood that the State Department does not get the C Series, but gets other Bulletin series. Who is to notify the State Department in the case of indications of compromise? As an example, take C-871 which shows that the Germans are apparently reading the Brown code. What action was taken on the part of the Signal Security Agency? Colonel Cook queried the State Department in this case and they stated it was Brown and "everybody knows Brown is only used for brevity purposes", but suppose it had not been Brown, but a high-grade system? Obviously, Cryptographic Branch has no power over the State Department. Whose job is it to notify them?

7. Another example is the evidence obtained from ULTRA sources which shows that the Japs are reading French systems; in some cases, messages in these systems contain data about our troop movements, etc. (See special report on this matter.) Whose responsibility is it to put a stop to this sort of leakage of important information?

8. There are indications that the Japanese have been reading some Allied messages which contain false information (see MIS special report). In order to properly evaluate this material, Allied deception programs must be known.

9. All these are matters that require G-2, Joint Security Control, Security Division, Intelligence Division, State Department, and SHAEF coordination as well as coordination with the various theatres. At present, there are many loose ends with no definite procedure being followed. No mechanics are set up for informing the right people at once. The responsibilities of the Signal Security Agency and those of G-2 should be clearly set forth.

II. IT IS RECOMMENDED THAT

1. Signal Security Agency evaluate all evidences of cryptographic compromises.

2. Through liaison with G-2, collateral material necessary for checking and amplification of the evidence be obtained through the channel already authorized. Messages of inquiry to theatres requiring coordinated action between G-2 and SSA will frequently be necessary.

3. Signal Security Agency take the necessary action in cases where cryptographic compromise is indicated of War Department systems over which it has direct control.

4. In cases over which it does not have direct control, Signal Security Agency pass the results of its evaluation of cryptographic compromise to G-2 through the same channel mentioned in paragraph 2 above, who will notify the theatres or organizations concerned. When necessary, identical messages will be sent by Signal Security Agency to the theatre or organization Signal Officers concerned.

5. In cases of Navy, State Department, or other U. S. Government agency, or Allied code compromise, Signal Security Agency likewise pass this information on to G-2 for necessary action, unless G-2 authorizes direct liaison between Signal Security Agency, State Department, and Navy in their particular fields.

6. At Signal Security Agency, the responsibility for the proper evaluation of cryptographic compromise indicated from ULTRA captured documents, and P/W reports be vested in one of three possible organizations:

a. The Security Division.

b. The Office of the Director of Communications Research, or

c. The Intelligence Division.

In any case, a full time job for a small unit with a definite T/O is necessary.

7. The evaluation authority prescribe the methods necessary for the proper screening of the ULTRA material available through check lists furnished to translators and the Bulletin Section. Some of these items should be:

a. All messages that emanate from certain message centers like "North Hiroshima Tsushinsho American Intelligence" messages.

b. All quotations from A, B, C, and D intelligence, as well as other obvious sources.

c. All traffic analysis references.

d. All references in addresses of Central Special Intelligence Bureau, any other Special Intelligence Bureau, Special Radio Unit, Special Signal Examination Unit, etc.

e. All quotations from communications of any sort.

f. All references to foreign cryptographic systems.

8. If translators are trained properly in such a check list, the messages falling in the above categories be placed in the C series, otherwise, the C series be abolished and scanning in I&L Branch should continue as at present. The messages in this series should be free of excessive use of Kana, and explanatory footnotes should be used freely.

9. If the C series is continued, its distribution be revised to permit their inclusion in other Signal Security Agency and G-2 studies, since there are times when the lack of particular messages prevents complete studies being made.

10. The evaluation authority have access to the Diplomatic and Far East Summaries.

11. All Allied deception programs using signal communications for the sending of false information in plain or code text, or the use of dummy traffic, be made known to the evaluating unit. If compromised code or cipher methods are used for the transmission of this false material, such methods must have the joint approval of Signal Security

Agency and [illegible]

12. In cases which indicate the reading of plain-text messages, studies be made by the evaluation unit. Where improper classification of the information has been made, G-2 will be notified as a matter for their information and action. If the plain text constitutes a compromise of similar information previously or later cryptographed, action will be taken by Signal Security Agency as indicated in paragraphs 3, 4, and 5 above.

13. Copies of all action cables sent and received in cases covered herein be exchanged between Signal Security Agency and G-2.