

MEMO ROUTING SLIP		NEVER USE FOR APPROVAL, CONCURRENCES, OR SIM.		APPROVALS, ACTIONS	
1 NAME OR TITLE		INITIALS		CIRCULATE	
ORGANIZATION AND LOCATION		DATE		COORDINATION	
2				FILE	
				INFORMATION	
3				NECESSARY ACTION	
				NOTE AND RETURN	
4				SEE ME	
				SIGNATURE	
REMARKS					
<p>For material subsequent to this on French COMSEC, see file folder "USCIB 23/- ALLIED (NATO) COMSEC"</p>					
FROM NAME OR TITLE		DATE			
ORGANIZATION AND LOCATION		TELEPHONE			

Declassified and approved for release by NSA on 03-07-2014 pursuant to E.O. 13526

~~SECURITY INFORMATION~~ ~~TOP SECRET CANOE~~ MAY 1953

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE~~HISTORY

15 MAY 1953

EO 3.3(h)(2)
PL 86-36/50 USC 3605EO 3.3(h)(2)
PL 86-36/50 USC 3605

1.a. Early Consideration: In 1948 USCIB discussed the problem of [redacted] as the most important aspect of the "Security of Western European Union Consideration." USCIB could not agree on measures to be taken and submitted to the National Security Council (NSC) a split report: the majority (ID, ASA, CNC, and CIA) feeling that [redacted] communication insecurity. NSC voted to take no action but to keep the problem under surveillance.

b. It may be noted at that time that [redacted] wanted to reveal to the [redacted] systems and [redacted] so expressed himself to Marshall, but Marshall replied that NSC could not accept the [redacted] proposal.

2.a. Reconsideration of Problem 1950: The problem was raised again in USCIB in September 1950 when the seriousness of the situation was felt by CIA and the Department of State to merit reconsideration.

b. SECCOM to which the problem had been referred submitted its report to USCIB in November 1950 recommending that steps be taken to improve [redacted]

c. On 12 December 1950 a letter was received from LSIB giving the British views on the subject of the [redacted] cations. The letter stated that the British were of the opinion that a [redacted]

d. In late January 1951 Admiral Stone appointed an AFSA Ad Hoc Committee under the chairmanship of Mr. William F. Friedman to work out a draft of the US position on the matter. This committee submitted on 7 February its report, the main conclusions of which were: [redacted]

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~ is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

c. This situation can be corrected only by a complete overhaul and replacement of the present insecure cryptographic systems by secure systems.

d. The importance of [redacted] to Russia is such that it is in the interest of the United States not only to accept a similar denial for itself, but to provide, at least in part, the cryptographic devices essential to security.

e. Negotiations with the [redacted] should be conducted in such a manner that [redacted]

f. Negotiations with the [redacted] should, if practicable, be conducted entirely by the [redacted] in order to avoid disclosure of BRUSA [redacted]

g. Negotiations should not be instituted prior to the formation of a secure group within the [redacted] Government."

e. On 13 March 1951 a letter was sent to LSIB proposing the agenda for the forthcoming conference within the framework of overall [redacted] security. The points of the agenda were:

- "1. The nature and scope of the insecurity of [redacted] communications, including both [redacted] communications.
2. The nature and scope of present [redacted] internal insecurity.
3. The most effective technical assistance which can be given to the [redacted].
4. The development of a specific plan for improvement of [redacted] communications insecurity.
5. The basis for a successful approach to the [redacted] Government."

The letter also stated the composition of the US delegation.

f. [redacted] proposals for the Conference were received 13 April 1951. These were accompanied by data which were concerned with both diplomatic and non-diplomatic [redacted] and which were more comprehensive and detailed than had been drawn up by the US.

~~TOP SECRET CANOE~~

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

j. The [] Conference was held 1-14 May 1951 in Washington. Its recommendations were

- "a. The above conclusions be approved;
- b. The proposed approach and plan be implemented when LSIB and USCIB have agreed that the requisite conditions have been met;
- c. The respective Chairmen of LSIB and USCIB and/or their nominees visit [] in order to brief the U.K. and the U.S. Ambassadors and also to participate as required;
- d. LSIB and USCIB keep this problem under continuous review, and take such implementing action as may be agreed to be necessary;
- e. The U.K. Government provide eight and the U.S. Government twelve of the twenty CCMs required for initial implementation of the cryptographic plan, and that the additional sixty CCMs be provided by the two Governments in a program phased in consonance with their respective NATO commitments."

4. Action by USCIB:

a. On 24 May, 1951 the Report of the Conference (USCIB: 14/132) was discussed and approved by USCIB, which also agreed to submit it to the National Security Council (NSC) for approval of the recommendation to approach the [] and of the conditions precedent thereto

b. At this meeting USCIB also appointed an ad hoc committee, composed of the members of the U.S. delegation to the US/UK Conference on [] Security, to keep developments pertaining to [] under continuous review, and to advise USCIB of the appropriate time for taking further action.

5. LSIB action: LSIB approved the report on 7 June 1951, in a memorandum to the Chairman, USCIB, in which the Chairman, LSIB stated further that LSIB "has decided that it does not require the approval of any higher authority." (TAB 1)

6. Action by NSC: The Chairman of USCIB submitted the Report to the NSC on 8 June 1951; on 11 January 1952 the President approved its conclusions and recommendations.

7.a. Paragraph 3k of the Report of the [] Conference states that:

"Since the report of the Tripartite Group now studying the internal security of the [] Government may well add to our knowledge in this regard, any approach to the [] should be deferred pending consideration of that report."

b. In August 1951 the Report of the Tripartite Working Group was approved by the U.S.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE~~~~TOP SECRET CANOE~~

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

8. In a memorandum to the Chairman, USCIB, dated 10 December 1951 (USCIB: 14/185) the Chairman ISIB stated that "ISIB has now examined the

[redacted]

ISIB further proposed that the approach be made "at the first opportunity" and stated that the "UK authorities can provide in two months' time 8 CCM machines to be offered [redacted] (as per the recommendation in paragraph 4e of the Report). Appendix A to ISIB's Memorandum sets forth the details of ISIB's proposed briefing of the US and the UK Ambassadors [redacted] (as per last sentence of sub-paragraph a above). ISIB now wishes USCIB's comments on its proposals "at its earliest convenience." (TAB 2)

9. On 14 January 1952, USCIB informed ISIB that NSC had approved the US/UK report. (TAB 3)

10. The matter of [redacted] was raised at the 73rd Meeting of USCIB on 18 January 1952. TAB 4 is the brief presented by Mr. Friedman at this meeting.

11. On 24 January 1952, USCIB informed ISIB by a letter (approved by USCIB at the 73rd meeting) that it was agreed at the Conference that an

[redacted]

letter further stated that it was the understanding of USCIB that an approach to the [redacted] should not be made until the Tripartite Report had been approved by each of the participating countries and the [redacted] Government had undertaken definite implementing action on the basis of its approval. (TAB 5)

12. On 18 April 1952, the matter of [redacted] was raised at the 76th Meeting of USCIB. It was pointed out that final British approval with no exceptions of the Tripartite Security Report had been received on 25 March 1952. With regard to the [redacted], no final approval had been received, however, it was believed that the [redacted] would be ready for a Tripartite meeting as early as 15 May 1952 (USCIB 23/45) (TAB 6)

13. On 13 February 1953, USCIB agreed that representatives of the Department of State and Department of the Army would coordinate with the Director, NSA, in the preparation of a report to USCIB on the importance and frequency of security violations by various allied nations based on an analysis of their transmissions. (USCIB 23/46) (TAB 7)

14. On 26 February 1953, ISIB, in a letter to USCIB, proposed that a conference be held on the subject of [redacted] Security. (TAB 8)

15. On 18 April 1953, USCIB replied, agreeing to conference and requesting a suggestion of a suitable opening date subsequent to the middle of May. (TAB 9)

16. Tab 10 contains information which may be useful in considering [redacted] COMINT potential, as reported by [redacted] as a result of a visit on 16-18 Feb 1953 to [redacted] 437.

EO 3.3(h)(2)
PL 86-36/50 USC 3605