

~~TOP SECRET SUEDE~~~~SECURITY INFORMATION~~~~CONFIDENTIAL INFORMATION~~

17 January 1952

~~TOP SECRET SUEDE~~EO 3.3(h) (2)
PL 86-36/50 USC 3605USCIB Meeting to be held on 18 January 1952Briefing Sheet on Item 3[] Communication Security (USCIB: 14/185 and 188)

1. The events and considerations which resulted in a [] Conference on [] Communication Security, held at Washington in May 1951, are set forth in the Enclosure.

2. On 27 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.

3. The Chairman of USCIB submitted the Report to the NSC on 3 June 1951; on 11 January 1952 the President approved its conclusions and recommendations.

4.a. 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." He also stated that "a draft brief to the [] is being prepared for discussion between representatives of our two Boards."

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

U.K. making an initial approach to them about their communication security." LSIB further proposed that the approach be made "at the first opportunity" and stated that the "UK authorities can provide in two months' time 8 COM machines to be offered to the [] (as per the recommendation in paragraph 4e of the Report). Appendix "A" to LSIB's Memorandum sets forth the details of [] to [] (as per last sentence of sub-paragraph a above). LSIB now wishes USCIB's comments on its proposals "at its earliest convenience."

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

[]

report."

~~TOP SECRET SUEDE~~EO 3.3(h)(2)
PL 86-36/50 USC 3605

b. In August 1951 the Report of the Tripartite Working Group was approved by the US. As of this date neither the [] nor the [] Government has approved that Report. However, it is to be noted that despite the conclusion quoted above in sub-paragraph a, the pertinent recommendation based upon that conclusion simply states that: (USCIB:lh/132,bb)

"b. The proposed approach and plan be implemented when LSIB and USCIB have agreed that the requisite conditions have been met."

c. It appears, therefore, that the recommendation of the []

6. With reference to the CCM's to be provided, the UK, as noted above, will be ready in about two months to provide its quota (8) of the twenty machines initially required for the []; the US agreed to furnish the remaining twelve. At the time of the Conference, the Army agreed to provide these twelve machines and it is assumed that this promise is still valid. Sixty additional machines are to be provided by the US and the UK "in a program phased in consonance with their respective NATO commitments."

W.F.F.

~~TOP SECRET~~~~TOP SECRET~~

~~TOP SECRET SUEDE~~
~~SECURITY INFORMATION~~SECURITY INFORMATION

17 January 1952

~~TOP SECRET SUEDE~~ENCLOSUREEO 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 too much [redacted] would be lost to the US by informing the [redacted] [redacted] NSC voted to take no action but to keep the problem under surveillance.

b. It may be noted at that time that Great Britain wanted to reveal to the [redacted] and [redacted] so expressed himself to Marshall, but Marshall replied that NSC could not accept the British 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] only when a secure group had been established within the [redacted] Government which could receive information without risk of compromise. The provision by the US or UK of a cryptographic system for [redacted] was recommended as the best solution.

c. On 12 December 1950 a letter was received from LSIB giving the British views on the subject of the insecurity of [redacted] communications. The letter stated that the British were of the opinion that a complete reorganization of the [redacted] arrangements was necessary and that they were prepared to reveal to the French the fact that they could read [redacted] The letter further proposed that an AFSA/GCHQ Conference be held in early 1951 to work out the details of action required.

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:

"a. Much valuable intelligence is contained in the [redacted]

Enclosure to Briefing Sheet on Item 3 (73rd Meeting USCIB)~~TOP SECRET SUEDE~~EO 3.3(h) (2)
PL 86-36/50 USC 3605EO 3.3(h) (2)
PL 86-36/50 USC 3605EO 3.3(h) (2)
PL 86-36/50 USC 3605

~~TOP SECRET SUEDE~~
~~TOP SECRET SUEDE~~

EO 3.3(h) (2)

PL 86-36/50 USC 3605

~~TOP SECRET SUEDE~~

b. The present cryptographic systems and practices of the [redacted] /are such that this intelligence is fully available to any efficient communication intelligence (COMINT) organization.

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 denying this source of COMINT 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 there is [redacted]

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

EO 3.3(h) (2)

PL 86-36/50 USC 3605

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]. The points of the agenda were:

1. The nature and scope of the insecurity of [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. British proposals for the Conference were received 13 April 1951.

EO 3.3(h) (2)

PL 86-36/50 USC 3605

~~TOP SECRET~~~~SECRET~~TOP SECRET SUEDE

g. The US/UK 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 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."

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

~~TOP SECRET~~~~SECRET~~