First Meeting of the Ad Hoc Committee
Appointed by DIRAFSA to Consider
The Problem of French Security

25 January 1951 - 1400
Conference Room - NSS

Mr. William F. Friedman, Chairman

Members: Captain T. H. Dyer, USN
Mr. F. B. Rowlett
Dr. A. Sinkov

Secretary: Mr. H. D. Jones

Also Present: Mr. H. S. Erskine
Mr. Frank Raven
Mr. Sidney Jaffe

The CHAIRMAN opened the meeting by outlining briefly the problem before the Committee. He referred the members to the papers distributed by the Secretary for more detailed information and background material.

1. Meeting at the State Department:

The CHAIRMAN informed the Committee that he had attended a conference on the French Security Problem at the Department of State the previous day. Those present included representatives from State, CIA, and the Assistant Chief of Staff, G-2, U. S. Army.

He reported that the discussion was concerned mainly with the method of presenting the security problem to the French, and was based primarily on a dispatch from Mr. Bruce, in Paris. Mr. Bruce was reporting a proposal made to him by the British that they, unilaterally, take up the matter with the French.

The CHAIRMAN outlined briefly a plan discussed at the meeting, which had the following features:

a. A Tri-partite working group - 4 members from each country - which would meet first in Washington or London, and rotate to the other locations, to study French Security standards, regulations and practices.

b. Should the French, in these conferences, bring up the matter of Communications Security, they would be told that it was outside the province of the discussions.

c. Only if the French gave concrete evidence that they would do something to improve personnel and physical security would there be a possibility of communications security being considered by this group.

2. General Comments on Problem Before the Committee:

The CHAIRMAN explained that USCIB had agreed to a conference with the British in late March or early April on the general COMSEC aspects of French Security. He stated that the Committee's problem was a technical one which involved recommending a plan of action to USCIB to be used as a U.S. basis in U.S./U.K. discussions.

3. Technical Aspects of French Cryptography:

MR. SIDNEY JAFFE, AFSA-232, was present to brief the Committee with a technical evaluation of the cryptographic systems, practices and procedures employed by the French Government. He reviewed briefly, for the Committee, the status of French Diplomatic, Army, Navy, Air, Police and Agent systems.

4. Conclusions Reached by the COMMITTEE:

From Mr. Jaffe's presentation, which included considerable detail and which pertained to military, as well as diplomatic cryptography, the Committee drew certain conclusions, among which were the following:

a. As a result of the place occupied by France in world affairs, and the inherent enthusiasm of the French in diplomatic activities, any insecurity in the handling of information available to the French leaders makes this government a prolific and valuable source for USSR intelligence operations.

b. There is concrete evidence that the French have used, and continue to employ, insecure methods in the handling of information.

c. One of the most significant examples of French insecurity lies in the nature of their cryptographic systems and the manner in which they are used.

(1) The majority of their cryptosystems are inherently insecure.

(2) There appears to be no clear-cut rule for the use of a particular system for particular information.

(3) Cryptographic discipline is poor, there being no evidence of a strictly-enforced plan to insure correct cryptographic procedure.

(4) Cryptographic technicians are inadequately trained.

d. That any well-organized cryptanalytic organizations would have little difficulty in obtaining information from French traffic.

e. The few secure French cryptosystems, if used exclusively, would break down under the current volume of French traffic.

f. The end alternative requires that the French be provided, in some manner with adequate cryptographic facilities and training.

5. Committee Decisions:

a. That there be prepared by AFSA-02, for forwarding with the Committee's final report, a brief statement on the technical aspects of French cryptography.

b. That the Committee meet again on 26 January 1951, in Room 2029-A,

Arlington Hall Station, at 0900, to consider the assigned problem further. AFSA-02 representatives agreed to have information available on the cryptographic security of other NATO nations.

H. D. JONES
Secretary,
Ad Hoc Committee