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

30 January 1951 - 0900
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 referring to an extract from the tentative minutes of the Fifty-ninth USCIB Meeting. He said that he thought these minutes, which pertained to the French problem, would be of interest to the committee members, and asked the Secretary to distribute copies.

The members agreed to postpone, until later in the meeting, consideration of the "Tentative Draft" on technical aspects of the French problem, and proceeded with a discussion of the specific cryptographic systems which merited consideration for use by the French in a revised cryptographic plan for diplomatic communications.

As a result of this discussion, the committee agreed upon a cryptographic plan which, in general, provided that the holders of French Diplomatic Systems be divided into three categories, according to the level of their communications. The systems recommended included the CCM, the

M-209 with special and general settings, one-time pads, and literal code books - emphasis being given to systems with which the French were familiar. Mr. Sinkov agreed to have this cryptographic plan written up for the next meeting.

The members then discussed the general form of the report to be submitted by the committee. It was agreed that the report would be in the form of a staff study, and CAPTAIN DYER agreed to prepare a draft report for circulation and consideration at the next meeting.

The "Tentative Draft" on technical aspects of French Cryptographic Security was reviewed and certain amendments were proposed and accepted. It was agreed that the final form of this paper would be included as a part of the Committee Report.

MR. ROWLETT distributed copies of the AFSA-02 evaluation of the cryptographic capabilities and security practices of NATO nations other than France. This paper was not considered in detail.

It was agreed that the next meeting of the committee would be held in the same room at 0900, Saturday, 3 February 1951.

H. D. JONES
Secretary,
Ad Hoc Committee