STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. Friedman, AFSA-00T DATE: 25 Jan 51

FROM : Mr. Rowlett, AFSA-02A2

SUBJECT: Attached drafts

Herewith are 3 copies of the draft paper you asked me for yesterday. The attached copies are for you, Dr. Sinkov, and Mr. Jones. I have given Capt. Dyer a copy myself.

TENTATIVE DRAFT

2. From an over-all consideration it is concluded that if the French Diplomatic cryptographic systems are to be improved ~~the following is~~ it would be to necessary:

a. Replace the current French Diplomatic Systems with secure systems;

b. Provide adequate training in the new systems for French cryptographic personnel;

c. Establish appropriate communications security procedures in the French Foreign Office;

d. Maintain careful technical supervision over the French Diplomatic communications.

3. In regard to the current French systems, it is concluded that observed French cryptographic practices in system design and distribution provide direct evidence that the present cryptographic organization does not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security. It is also concluded that, except as regards the infrequently used one-time pad systems, none of the French Diplomatic cryptographic systems possess sufficient inherent security to permit improvement to a point where it may be considered acceptable. It is therefore necessary to discard the current systems and replace them with other systems based on better cryptographic principles.

4. In regard to 2b, 2c, and 2d above, the current practices of the French show a lack of appreciation on their part of the importance of these points to communications security. It is felt that able technical assistance from outside the French Diplomatic cryptographic service will be required if adequate measures are to be inaugurated in regard to these points.

5. In view of the foregoing, it is concluded that a complete "house-cleaning" of the French Cryptographic Service would be necessary. This would involve not only informing the French that their present systems are considered insecure but also establishing a basis on which the French would be provided with appropriate technical assistance to enable them to

reorganize their cryptographic service to insure secure handling of communications.

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

[redacted]

7. The British in the past have had many contacts with the French cryptologists. It appears advantageous that, if the French are approached on this matter, it be ~~effected~~ done unilaterally and initially ~~(on a unilateral basis)~~ by the British.

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

Such a course of action would present the additional advantages that it ~~since it~~ (a) ~~would not need to indicate~~ would be unnecessary to disclose the [redacted] (b) limit the number of ~~technical personalities~~ technicians who it would [redacted]

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

agencies are the only losers. If, however, the French are only partially penetrated, the action discussed above will be of advantage in that it will localize and consequently reduce the amount of ~~minimize the~~ information obtained by the Russians from COMINT operations.

Secret