3 July 1950

MEMORANDUM FOR DIRAFSA

Subject: U.S.-British Interchange of Cryptographic Principles on a Reciprocal Basis.

1. The following personnel met on 30 June 1950 to recommend types of equipment and developments to be discussed with the U.K. representatives:

Colonel Collins
Captain Safford
Mr. Friedman
Dr. Sinkov
Captain Shepard
Dr. Kullback
CDR Enderlin (for Item a only)

2. It was recommended that the following equipments be discussed under each of the categories listed below:

a. Special purpose teleprinter systems for the exchange of intelligence material.

ASAM 2-1 bK
[redacted]

b. Low echelon (minor war vessels) telegraphic systems.
c. Merchant ship telegraphic systems.

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

PCM
*AFSAM-7
MCM
[redacted]
Paper and pencil system
Strip systems

d. Meteorological security systems including facsimile, teleprinter and telegraph.

ASAX-2
NRL Cifax
[redacted]
CSP 3800A
PCM
*AFSAM-7
ASAM 2-1

e. Voice security systems for tactical purposes.

Mr Scott - 11

Y-9
Y-4
Buker low-echelon ciphony system

*These items were considered applicable but it was generally agreed that they should not be disclosed to U.K.

3. It is recommended that the above list and agenda of equipment to be discussed be submitted to AFSAC and at that time ask that two representatives from each Service be designated to attend the conference.

S. P. COLLINS
Colonel, Signal Corps
Deputy Director, AFSA

2 Incls
1. Memo to COA from 14 dated 22 June, subject as above.
2. Brief description of equipments

SERVICE	SHORT TITLE	DESCRIPTION
(A)	ASAM 2-1	Teletype cipher device used with 131B2 subset table. Modified Army ASAM-1 or Navy CSP-1500.
(A)	AFSAM 7	Converter MX-507()/U. Low echelon, electro-mechanical off-line cipher equipment.
(A)	AFSAM 9	General purpose teletype cipher machine.
(A)	AFSAM-15	Fully synchronous teletype cipher machine for aircraft movement system.
(N)	AFSAM-33	Teletype cipher equipment, off line.
(A)	ASAX 2	Facsimile security equipment for enciphering weather maps.
(N)	CSP 3800A	Modified CSP-3800 to provide encipherment of digits for weather traffic.
(N)	MCM	Mechanical Cipher Machine for low echelon literal requirements.
(N)	PCM	Portable Cipher Machine for low echelon use where electrical power is available.
(A)	Y-9	Staff level ciphony system to provide speech security over short circuits serving various Staff Commands.
(A)	Y-4	Low echelon speech security system.
(N)	NRL Cifax	Facsimile security equipment for the encipherment of weather maps.

STANDARD FORM NO. 64

REF ID:A67307

Office Memorandum • UNITED STATES GOVERNMENT

TO : OO

DATE: 23 June

FROM : OOA

SUBJECT: Agenda for US-UK Conference

If you concur I will have a list of conferees made up for your approval

OOA

Yes - I think, however, this matter will have to be coordinated with JCEC - or possibly be arranged by AFSAC Technical Committee in order to get coordinate with the Services. In any case, I have promised to get a tentative agenda to the Br. soon. EFS

TOP SECRET

MEMO ROUTING SLIP — APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE: Col. Collins	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION: OOA	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

1. Herewith draft agenda you requested in your memo of 14 June 1950.

2. I have made no recommendations as to the specific machines, devices, or systems to be disclosed, because I feel that that should be the first job of the U.S. representatives to decide on in their pre-conference meetings. I suggest that the U.S. representatives be nominated as per par. 4 of my covering memo, that they be directed to examine the draft agenda, make any recommendations for addition or deletions therein, and that they then submit for your approval a list of specific U.S. machines, devices, systems, principles, and/or components to be disclosed and discussed in BR-US conferences. That list need not accompany our proposed Agenda when the latter is forwarded to the British.

3. I presume that U.S. representatives will include personnel from AFSA, from the three Service Cryptologic Organizations, and from the Army (Signal

(over)

FROM NAME OR TITLE: W. F. Friedman		DATE: 22 June 50	
ORGANIZATION AND LOCATION: AFSA-14		TELEPHONE: 455	

NME FORM NO 95 1 OCT 48 Replaces DA AGO Form 895, 1 Apr 48, which may be used. 16-28487-8 GPO

TOP SECRET

Corps), the Navy (Naval Communications) and the Air Force (Air Communications). In the case of item 1a of the Agenda, AFSA representatives must include people who can present the interests of AFSA-02 and AFSA-13. In the case of item 1d, it is possible that there may have to be people who can present the interests of the meteorological agencies of the Services, but this can be ascertained later.

4. AFSA-14 will be glad to coordinate the preparation of recommendations for nominations of U.S. representatives.

J

MEMORANDUM

22 June 1950

TO: AFSA-OOA

FROM: AFSA-14

Subject: U.S.-British Interchange of Cryptographic Principles on a Reciprocal Basis

Reference: OOA Memo to AFSA-14 dated 14 June 1950

1. Attached is a tentative agenda for the subject conference as requested by reference.

2. If completely free discussion on the part of the U.S. conferees is permitted on the five subjects, the deliberations of the conference will almost certainly spread to virtually all U.S. cryptographic principles and equipments now under development or in the idea stage at AFSA. For example, a complete discussion on the first item, special purpose teleprinter systems for the exchange of intelligence material, might well involve the ASAM-9 and the ASAM-15. The second item, minor war vessels systems, might involve a discussion of the PCM and the ASAM-7. If the ASAM-7, 9 or 15 are discussed, then the 36-point rotor and the re-entry principle have to be disclosed. Another example is in the case of ciphony equipment. Our knowledge on ciphony systems for tactical use comes in a large part from higher level developments which are not on the agenda. In short, if this is to be a limited conference, as intended by the U.S., then the limitations must be clearly defined. The only possible or practicable way to do this would be to require the U.S. conferees to confine their discussions to specific equipments, without going into or giving background reasoning if the latter involves ideas not to be disclosed. The specific equipments and ideas to be disclosed and those to be withheld must be clearly set forth prior to the conference.

3. From a purely technical viewpoint, of course, a very strictly limited conference is much less satisfactory than a completely unlimited one. A more serious consideration, if the conference is to be very limited, is that the U.S. may be put into an embarrassing position at a later date if the British should adopt some of the U.S. developments disclosed at this conference, while the U.S. subsequently chooses to adopt equipments withheld. For this reason, it would be advisable to inform the British that the U.S. is not committing itself to utilize any of the equipments now under development which are being disclosed.

Memorandum to AFSA-OOA (continued)

4. In view of the comments made above, it is suggested that the U.S. representatives to this proposed conference should be nominated at an early date and meetings of these representatives should be held prior to submission of the agenda to the British and certainly prior to the first meeting. The purpose of these meetings of purely U.S. representatives would be to clarify the situation by establishing and defining the limitations on discussions with the British in the Combined Conference.

5. It is suggested further that the conference be organized in sub-committees, one for each of the five items on the agenda, and an executive committee with a procedure similar to previous BRUSA technical conferences.

6. AFSA-03, 04, and 12 are in essential agreement with the above and with the proposed agenda.

William F. Friedman

WILLIAM F. FRIEDMAN
Chief, Technical Division

Incl
Tentative agenda

Agenda for U.S.-British Conference
on the Exchange of Cryptographic Principles

Reference: Memorandum from OOA dated 14 June 1950

1. The subject conference is to be an initial exploratory conference to exchange information by disclosure of models and designs of cryptographic equipment now under development in the following categories:

a. Special purpose teleprinter systems for the exchange of intelligence material.

b. Low echelon (minor war vessels) telegraphic systems.

c. Merchant ship telegraphic systems.

d. Meteorological security systems including facsimile, teleprinter and telegraph.

e. Voice security systems for tactical purposes.

2. It is suggested that each of these types of systems be discussed according to a pattern such as that outlined in enclosure A.

Enclosure A

Discussion of

I. Desirable [redacted] Characteristics -

A. General

1. Objective

2. Type or level of Employment

B. Operational Characteristics

1. Security

a. Cryptosecurity

b. Radiation Security

c. Transmission Security

2. Functional Requirements

3. Radio Interference

4. Power Requirements

5. Special Requirements

C. Physical Characteristics

1. Weight and Volume Factors

2. Operation, Transportation, Packaging and Storage Requirements

3. Destruction Requirements

D. Operation and Maintenance Characteristics of Equipment

E. Comint Implications with Respect to Consequences of Capture of Equipment

II. Present Equipment - U.S.

A. Demonstration or Description

B. Discussion concerning Adequacy According to I (Interim, Long-range, Emergency).

Enclosure A (continued)

III. Present Equipment - U.K.

A. Description or Model Demonstration

B. Discussion concerning Adequacy According to I.

IV. Equipment under Development - U.S.

A. Description or Model Demonstration

B. Adequacy according to I

C. Present Status

D. Plans

V. Equipment under Development - U.K.

A. Description or Model Demonstration

B. Adequacy according to I

C. Present Status

D. Plans