~~SECRET~~ ~~SECURITY INFORMATION~~

~~SECRET - SECURITY INFORMATION~~

SUBJECT: 1953 UK/US COMSEC Conference

TO: P/P FROM: C/SEC DATE: AUG 3 - 1953 COMMENT NO. 3
FCAustin/60489/ebs

1. General subjects for the agenda (Phase 1) are as follows:

a. Security of cryptosystems previously discussed in UK/US COMSEC Conferences and still under active consideration in the US, UK, or both.

b. Security of PANDORA, BALDER, MERCURY, HERCULES, and AFSAW 7224. These have not been discussed in earlier BRUSA COMSEC Conferences.

c. Security standards.

2. The general objectives are exchange of information on each cryptosystem considered, determination of the degree of security it affords, discussion of means of improving its security where such is desirable, and arrival at agreement on the level of use for which it is acceptable. Security standards are to be discussed with the aim of arriving at a common set of standards in judging the security of cryptosystems.

3. A list of papers and reports already forwarded and to be forwarded is supplied as Inclosure 1.

4. General subjects for the agenda (Phase 2) are as follows:

a. CCM replacement.

b. Combined and NATO weather requirements.

c. On-line Combined and NATO requirements.

d. NATO second level back up (possible replacement of NATEX for this).

e. Remaining Combined NATO naval requirements (NCSC's and merchant shipping).

f. Remaining Combined and NATO tactical requirements.

g. Miscellaneous requirements such as IFF.

5. The objective of this phase will be to agree on equipment or systems to meet requirements.

6. The following persons are nominated as C/SEC's delegation to the conference: (It should be noted that the representation is so arranged that only two need stay for the entire conference. It should also be noted that, as agreed last time, there will be meetings on production agreements and on COMSEC procedural matters during

S/ASST

5

~~SECRET~~

SUBJECT: 1953 UK/US COMSEC Conference

DATE: AUG 3 - 1953 COMMENT NO. 3 (Contd.)

the conference (beginning in the preliminary informal phase) and that adequate representation is necessary for them as well as for the conference itself.)

a. Mr. K. Kuhn - NSA-42. Mr. Kuhn would be present only for the preliminary phase. He would be involved in the preliminary engineering discussions, in the trips to UK production and engineering facilities in the production agreement conferences. This opportunity for the Chief of the Crypto-Engineering Division to witness UK production methods at first hand will be extremely beneficial. He would return to the US approximately 28 October.

b. Mr. Ryon A. Page - NSA-412. Mr. Page would attend only for the preliminary security discussions and for the first part of Phase 1 of the conference proper. There are to be some 50 different items of cryptosecurity consideration and Mr. Page is principally responsible for the preparation of the US papers which have been and are being prepared on these items. Mr. Page would stay until about 1 November. (Note, for personal reasons Mr. Page might find it impossible to attend the conference; if such should occur Mr. Lowell Fraser (NSA-412) would go in his stead.)

c. Dr. Harold J. Stukey - NSA-412. Dr. Stukey would attend thru the first phase. As mentioned above there are an exceedingly large number of points to cover in the security field. Dr. Stukey would remain throughout Phase 1 in order to prepare the reports which will grow out of the informal phase and out of Phase 1 itself. He would return to the US approximately 5 November.

d. Mr. Thomas Chittenden - NSA-402. Mr. Chittenden would stay for the duration of the conference. During the preliminary and first stage he would attend the engineering trips and discussions. As representing the C/SEC Planning Staff he would participate in all the production discussions and agreements. During the second phase he would participate in the planning for meeting existing requirements. Probably the most difficult of the requirements which will come up is that of meteorological communications. As a member of the Combined weather security subpanel of the CAN-UK-US JCEC's Mr. Chittenden is particularly well qualified for this problem. It is also likely, the weather problem being so acute, that there will be weather meetings outside but during the conference itself.

e. Mr. F. C. Austin - NSA-41. Mr. Austin would stay for the duration of the conference. He would attend the security discussions in the preliminary and first phases, and would handle the US end of the procedures meetings. (We are on the verge of agreeing on a Combined and NATO crypto procedures manual (prepared by NSA-41 and CPB) but there are many questions which can only be resolved at the conference.) Mr. Austin would stay throughout Phase 2 since there will be many security and procedural questions arising during discussions of requirements. Mr. Austin also will have recently attended a NATO meeting on cryptographic matters and this should be of benefit in discussion of NATO requirements.

~~SECRET~~ ~~SECURITY INFORMATION~~

~~SECRET - SECURITY INFORMATION~~

SUBJECT: 1953 UK/US COMSEC Conference

DATE: AUG 3 - 1953 COMMENT NO. 3 (Contd.)

7. C/SEC strongly supports the suggestion made in paragraph 3 of Comment No. 2, that the sole criterion for disclosing equipments or cryptoprinciples to the UK in specific relation to this conference should be whether they are to be reserved for exclusive US use, except in those cases in which concurrence of a Service is required for disclosure of research and development under its cognizance. C/SEC's opinions on release of cryptoprinciples to the UK in general are contained in other correspondence addressed to you as comments to your D/F of 2 July.

F. E. HERRELKO
COLONEL, USAF
CHIEF, OFFICE OF
COMMUNICATION SECURITY

Incl:
US BRUSA Reports to be
Available for 1953 BRUSA
COMSEC Conferences, 29 July 53

~~SECRET - SECURITY INFORMATION~~

SUBJECT: 1953 UK/US COMSEC Conference

TO: C/SEC
S/ASST
P/P (IN TURN)

FROM: R/D

DATE: 20 JUL 1953 COMMENT NO. 2
Mr. JRChiles/jmr/60400

1. The following information in connection with the 1953 UK/US COMSEC Conference is supplied as requested in paragraph 3 of Comment No. 1.

a. General subjects for the agenda.

(1) Review of all equipments discussed previously, to include latest information on design changes since the last conference, results of further security evaluations, and current status of developments, in the following general categories:

Literal Cipher Machines
Teletype Security Equipments
Speech Security Equipments
Facsimile Security Equipments
Special Purpose Crypto-Devices
Crypto-Material Production Equipments
IFF and Data Transmission Security Systems

(2) Description of new U. S. developments authorized for disclosure to the U. K.

(3) Discussion of progress in material, component, and circuitry developments applicable to communication security equipments.

b. General objectives to be accomplished, as far as R/D is concerned, will be the continuation of a full and frank exchange of information and views on all agenda items covered, demonstrations of such equipments as can be made available, and the preparation of reports listing and assessing equipments available and under development.

c. Papers and reports prepared or in preparation within R/D for the conference include the following:

(1) Addenda to BRUSA C/S Nos. 1 through 42 and 201 through 211, where appropriate to bring information contained therein up to date.

(2) Description of AFSAM 26 (Single Channel Synchronous Teletype Security Equipment)

(3) Description of AFSAM 37 (FOX Broadcast Teletype Security Equipment)

~~SECRET - SECURITY INFORMATION~~

SUBJECT: 1953 UK/US COMEC Conference (CONSENT NO. 2 continued)

(4) Description of AFSAX D505 (FOX Broadcast Cifax Equipment)

(5) Description of AFSAY D601 (Special Purpose Ciphony Equipment)

(6) Description of AFSAY D610 (One-for-Four Ciphony Equipment)

(7) Description of AFSAZ 7306 (1,650 bit per second Wireline Transmission Equipment)

(8) Description of AFSAZ 7308 (Halftone Cifax Adaptor)

(9) Description of OPREG (Relay Rotor Analog)

(10) Description of BISON (Binary Setting Generator)

(11) Report on IFF and Data Transmission Systems Studies (NRL and APCNC Proposals)

(12) Interim Report on Radiation Studies

(13) Report on Mod 3 Kolsen Key Generator Studies

(14) Report on Fibonacci Key Generator Studies

(15) Report on Pulsed Magnetic Core Devices

(16) Report on Ferro-Resonant Elements

d. The following R/D personnel are nominated for the U. S. Delegation:

Mr. H. C. Barlow
Mr. J. R. Chiles
Mr. M. M. Mathews
Mr. B. G. Erickson
Dr. W. H. Erskine
Mr. W. P. King (Alternate: Mr. F. D. Buck)
Mr. Frank Mitchell (Alternate: Mr. T. H. Witcher)

Of these nominees, it is felt that it will be necessary for only one or two of the first three-named individuals to remain for Phases I and II of the Conference itself. The other R/D representatives will participate only in the informal discussions between the engineering and security experts during the two-week

SECRET - SECURITY INFORMATION

SUBJECT: 1953 UK/US COMSEC Conference (COMMENT NO. 2 continued)

period before the formal Conference opens. The exact composition of the delegation will depend to some extent on the agenda items proposed by the British. For example, if the emphasis in the field of speech security is to be on pulse code and delta modulation systems, Mr. King, as the R/D expert in these fields, will attend; if, on the other hand, vocoder systems are to be discussed in detail, Mr. Buck will replace him. Similarly, depending on whether the discussions in the field of literal and teletype security equipment will involve primarily electronic or mechanical aspects, either Mr. Mitchell or Mr. Witcher will participate.

2. It is tentatively planned to demonstrate engineering models of the following U. S. COMSEC equipments:

AFSAM 9 (Teletype Security Equipment)
AFSAM D17 (Portable Mechanical Cipher Machine)
AFSAY D008 (Low Echelon Airborne Ciphony Equipment)

In addition to the models of equipment listed above, a series of recordings of various speech security systems, samples of bistable magnetic and ferro-resonant elements, and some films on equipment and document destruction will be presented.

3. The new equipments and general studies or investigations which are tentatively planned for disclosure to the U.K. under General Agenda Items 2 and 3 listed in sub-paragraph 1a are enumerated in sub-paragraph 1g, items (2) through (16). It is requested that appropriate action be taken to obtain authorization for the disclosure of these items and that R/D be informed of such authorization at the earliest possible date. Considerable thought has been given to the selection of these items and it is felt that, in each case, disclosure to the U. K. will be in the best interests of this country. It is suggested, therefore, that the determination be based solely on whether or not the equipment and/or the crypto-principle involved is to be reserved for exclusive U. S. use, or (in the case of the AFCRC proposals for IFF and Data Transmission systems) on Air Force concurrence in the disclosure of Cambridge Research Center work in those fields. Further information on any of the items listed may be obtained from the Communication Security Equipment Division, Office of Research and Development.

S. KULLBACK Acting
Assistant Director
Research and Development

~~SECRET - SECURITY INFORMATION~~

~~SECRET - SECURITY INFORMATION~~

COPY

1953 UK/US COMSEC Conference

R/D P/P 1 July 1953 COMMENT NO. 1
C/SEC Mr. Douglas/421/gaw
S/ASST (IN TURN)

1. The 1953 UK/US COMSEC Conference is expected to be held in London about 1 October. The exact date has not yet been set by the Cypher Policy Board.

2. According to the recommendations of the 1952 Conference, the following conditions are to apply in the forthcoming Conference:

a. That a fortnight should be provided before the Conference opens for discussions between UK and US Engineering and Security experts for examination of equipments and for visits to establishments. Experience has shown that such exchanges can best be conducted informally.

b. That the Conference itself should be in the following two phases, held consecutively:

(1) Phase I: Preparation by the Engineering and Security Experts of reports listing and assessing equipments available and under development.

(2) Phase II: Meeting between US and UK communications staffs and representatives of C.P.B. and AFSAC to examine and define Combined and NATO operational requirements and, where possible, to recommend equipments to meet them.

3. It is requested that the addressees forward to this Division the following information:

a. General subjects for the agenda. Detailed items need not be included at this time but should be under consideration for later incorporation under the appropriate agenda item.

b. General objectives to be accomplished for each agenda item during the Conference.

c. A notation of papers and reports prepared or in preparation in support of agenda items.

d. Nomination of NSA personnel for the US Delegation.

4. Until a firm agenda is adopted, the foregoing information should be considered as tentative in nature subject to later revision.

JESSE O. GREGORY
Colonel, USAF

~~SECRET~~

~~SECRET~~ Security Information

~~SECRET~~ SECURITY INFORMATION

1953 UK/US COMSEC Conference

R/D
C/SEC
S/ASST (IN TURN)

P/P

1 JUL 1953

Mr. Douglas/421/gaw

1. The 1953 UK/US COMSEC Conference is expected to be held in London about 1 October. The exact date has not yet been set by the Cypher Policy Board.

2. According to the recommendations of the 1952 Conference, the following conditions are to apply in the forthcoming Conference:

a. That a fortnight should be provided before the Conference opens for discussions between UK and US Engineering and Security experts for examination of equipments and for visits to establishments. Experience has shown that such exchanges can best be conducted informally.

b. That the Conference itself should be in the following two phases, held consecutively:

(1) Phase I: Preparation by the Engineering and Security Experts of reports listing and assessing equipments available and under development.

(2) Phase II: Meeting between US and UK communications staffs and representatives of C.P.B. and AFSAC to examine and define Combined and NATO operational requirements and, where possible, to recommend equipments to meet them.

3. It is requested that the addressees forward to this Division the following information:

a. General subjects for the agenda. Detailed items need not be included at this time but should be under consideration for later incorporation under the appropriate agenda item.

b. General objectives to be accomplished for each agenda item during the Conference.

c. A notation of papers and reports prepared or in preparation in support of agenda items.

d. Nomination of NSA personnel for the US Delegation.

4. Until a firm agenda is adopted, the foregoing information should be considered as tentative in nature subject to later revision.

(signed)
JESSE O. GREGORY
Colonel, USAF

~~SECRET~~ Security Information