

~~TOP SECRET~~

REPORT TO THE BRITISH AND US CHIEFS OF STAFF
 BY THE BRITISH/US COMMUNICATION SECURITY EXPLORATORY CONFERENCE
 SEPTEMBER 1950

Initial exchange of Cryptographic Information under
 the following item headings:

- (a) Low Echelon (including Minor War Vessels) Telegraphic Systems including Combined Assault Codes and tactical systems for all military purposes.
- (b) Merchant Ships Telegraphic Systems.
- (c) Meteorological Security Systems, including Facsimile, Teleprinter and Telegraph.
- (d) Voice Security Systems for Tactical Purposes.
- (e) Teleprinter systems for the exchange of Communication Intelligence material.

* * * * *

1. As agreed by the British and the US Chiefs of Staff,* a British/US Conference to consider the above subjects was opened in Washington on the 21st September 1950.
2. Summaries of the proceedings at the meeting which followed have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London. In our estimation this conference has been of unquestioned value not only in the field of Combined Communications Security but also in the field of US and British

* US Reference: JCS 2074/2 - 27 December 1949.
 British Reference: COS(W)831 - 26 July 1950.

~~TOP SECRET~~

~~TOP SECRET~~**Intra-Communications Security.****3. It is recommended:**

- (a) That immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this conference. This should include technical visits.
- (b) That discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, be authorized.
- (c) That security evaluations be made and exchanged on all items discussed.
- (d) That the U.S.-U.K. JCEC consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.
- (e) That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time.

4. The general recommendations in paragraph 3 above together with the detailed conclusions of the Conference which are attached as Appendix A to this report are submitted for the approval of the British and U. S. Chiefs of Staff.

~~TOP SECRET~~

~~TOP SECRET~~APPENDIX ACONCLUSIONS

A. Low Echelon (including Minor War Vessels) Telegraphic Systems including Combined Assault Codes and Tactical Systems for all Military Services

(1) No machine system is likely to be available for general combined use before 1954.

(2) If combined systems are required for any of the foregoing purposes in the interim period, some possible systems are:

Strip

Linex

Cursex

Playfex

Running Key Cipher

(3) To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months. Some possible devices are:

DUP 1

AFSAM 7

"PCM"

AFSAM 9

MCM

Concert

Rollick

~~TOP SECRET~~

~~TOP SECRET~~**B. Merchant Ship Telegraphic Systems**

A machine system of at least equivalent security but faster than Cursex, which is under consideration, should replace it, when available, and that such a system should be selected within the next 12 months. Some possible devices are:

"PCM"

DUP 1

AFSAM 7

MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph

(1) No machine crypto system for meteorological purposes is likely to be available for general combined use before 1954.

(2) If combined systems are required for meteorological purposes in the interim period, some possible devices are:

(a) Air-Ground - ASAD 1

Otnetco

Alametco

(b) Telegraph - GCM (modified for weather encipherment) Pencil and paper system for very low echelon purposes.

(c) Teleprinter - ASAM 2-1

(d) Facsimile - None available

(3) To meet the long term requirements for encipherment of meteorological data, selection should be made within the next 12 months. Some possible devices are:

~~TOP SECRET~~

~~TOP SECRET~~**(a) Air-Ground - ASAD 1**

Otmotco

Alamotco

Any available ciphony system

**(b) Telegraph - 7 rotor BCM with provision for
weather encipherment**

AFSAM 7

"PCM"

Singlet

Pendragon

DUP 1 - designed for weather
encipherment

Pencil and paper systems

(c) Teleprinter - AFSAM 9

ASAM 2-1

Concert

Rollick

Mercury

(d) Cifax - ASAX 2

NRL Cifax

METFAX

NOTE: Selection in category (d) may not be possible until an agreement is reached in the UK-US JOEC on the requirements and characteristics for plain text facsimile equipment and associated transmission systems for meteorological use.

~~TOP SECRET~~

~~TOP SECRET~~**D. Voice Security Systems for Tactical Purposes**

(1) No ciphony system is likely to be available for general combined use before 1954.

(2) There are no possibilities for suitable devices in the interim period.

(3) To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. Some possible devices are:

- (a) ASAY 4 (primarily designed as a low echelon ciphony attachment; can be used only over circuits of normal band width)
- (b) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)
- (c) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)
- (d) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)

~~TOP SECRET~~

~~TOP SECRET~~

- (e) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)
- (f) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)
- (g) TSS (primarily designed for air-to-air and air-to-ground voice privacy system with minimum security of 20 minutes. Will operate with any existing U.S. aircraft voice transmitter or receiver, on frequencies as low as 175 KCS)

E. Teleprinter Systems for the Exchange of Communication Intelligence Material

- (1) If there is to be an immediate substitution for ROCKEX a selection can be made from the following machines:
- ASAM 2-1
5 U.C.O.
- (2) Either machine is available in sufficient quantity to meet current requirements in the exchange of intelligence material.

~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A67186

REPORT TO THE BRITISH AND US CHIEFS OF STAFF
BY THE BRITISH / US COMMUNICATIONS SECURITY CONFERENCE
SEPTEMBER 1950

EXPLORATORY

Initial Exploratory Conference for the exchange of
Cryptographic Information under the following item headings:

- (a) Low Echelon (including Minor War Vessels) Telegraphic Systems including Combined Assault Codes and tactical systems for all military purposes.
- (b) Merchant Ships Telegraphic Systems.
- (c) Meteorological Security Systems, including Facsimile, Teleprinter and Telegraph.
- (d) Voice Security Systems for Tactical Purposes.
- (e) Teleprinter systems for the exchange of Intelligence material.

Communications

* * * * *

1. As agreed by the British and the US Chiefs of Staff,* a British/US Conference to consider the above subjects was opened in Washington on the 21st September 1950.

2. Summaries of the proceedings at the meeting which followed have been prepared and these are held both by the Director, Armed Forces Security Agency, Washington, and the Secretary, Cypher Policy Board, London.

In our estimation this conference has been of outstanding value not only in the field of Combined Communications but also

Security

* US Reference: JCS 2074/2 - 27 December 1949.
British Reference: COS(W) - 25 August 1950.

Declassified by NSA/CSS

~~TOP SECRET~~

Deputy Associate Director for Policy and Records

On 20130819 by BF

~~TOP SECRET~~

Intra-Comm Sec *Security*
 in the field of US and British Intra-Communications, and we

It is recommended that
 3, ~~would make the following general recommendations:~~

- (a) ~~That~~ immediately and on a continuing basis, there be complete interchange of the technical details of the systems discussed in this exploratory conference. This should include technical visits.
- (b) ~~That~~ discussion and interchange of technical information on certain other items of combined interest, such as the security aspects of IFF and authentication systems, *key-tape generators* ~~mapping of documents~~ be authorized.
- (c) ~~That~~ security evaluations be made and exchanged on all items discussed.
- (d) ~~That a copy of the final report of the conference be submitted to the U.S.-U.K. JCEC and that the U.S.-U.K. JCEC be requested to consider and resolve as a matter of urgency the operational requirements in all fields of Combined Cryptographic Communications.~~
- (e) That there be annual conferences on these subjects for the next four years, to be held alternately in London and in Washington, the first of these to take place in London in approximately nine months time.

General
 4. The recommendations in paragraph 3 above together with the detailed conclusions of the Conference which are attached as Appendix A to this report are submitted *for the approval of* ~~with the recommendation~~ that they be endorsed by the British and U. S. Chiefs of Staff.

~~TOP SECRET~~

~~TOP SECRET~~APPENDIX ACONCLUSIONS

A. Low Echelon (including Minor War Vessels) Telegraphic Systems including Combined Assault Codes and Tactical Systems for all Military Services

(1) No machine system is likely to be available for general combined use before 1954.

(2) ^{Some} If combined systems are required for ^{of the foregoing} any purpose in the interim period, possible systems are:

Strip

LineX

Cursex

Playfex

Running Key Cipher

(3) To meet the long term requirements for low echelon combined systems selections should be made within the next 12 months. ^{Some} Possible devices are:

DUP 1

AFSAM 7

"PCM"

AFSAM 9

MCM

Concert

Rollick

~~TOP SECRET~~

~~TOP SECRET~~B. Merchant Ship Telegraphic Systems

A machine system of at least equivalent security but faster than Cursex, ^{which is under consideration} should replace it, when available, and that such a system should be selected within the next 12 months. ^{Some} Possible devices are:

"PCM"

DUP 1

AFSAM 7

MCM

C. Meteorological Security Systems, Including Facsimile, Teleprinter and Telegraph

(1) No machine crypto system for meteorological purposes is likely to be available for general combined use before 1954.

(2) If combined systems are required for meteorological purposes in the interim period, ^{Some} possible devices are:

(a) Air-Ground - ASAD 1

Otmeco

Alameco

(b) Telegraph - CCM (modified for weather encipherment) Pencil and paper system for very low echelon purposes.

(c) Teleprinter - ASAM 2-1

(d) Facsimile - None available

(3) To meet the long term requirements for encipherment of meteorological data, selection should be made within the next 12 months. ^{Some} Possible devices are:

~~TOP SECRET~~

~~TOP SECRET~~

(a) Air-Ground - ASAD 1

Otmeco

Alameco

Any available ciphony system

(b) ~~7-7-71 BOM (Ciphony system)~~
Telegraph - ~~BOM-7~~ with provision for weather

encipherment

AFSAM 7

"PCM"

Singlet

Pendragon

DUP 1 - designed for weather

encipherment

Pencil and paper systems

(c) Teleprinter - AFSAM 9

ASAM 2-1

Concert

Rollick

Mercury

(d) Cifax - ASAX 2

NRL Cifax

METFAX

NOTE: Selection in category (d) may not be possible until an agreement is reached in the UK-US JCEC on the requirements and characteristics for plain text facsimile equipment and associated transmission systems for meteorological use.

~~TOP SECRET~~

~~TOP SECRET~~D. Voice Security Systems for Tactical Purposes

(1) No ciphony system is likely to be available for general combined use before 1954.

(2) There are no possibilities for suitable devices in the interim period.

(3) To meet the long term requirements for combined ciphony systems selection should be made within the next 12 months. ^{Some} Possible devices are:

- (a) ASAY 4 (primarily designed as a low echelon ciphony attachment; can be used only over circuits of normal bandwidth)
- (b) ASAY 8 (designed primarily for airborne use; possibly suitable for general low echelon use; can be used with VHF transmission only and is capable of group working)
- (c) Hallmark (primarily designed for tactical point to point circuits using VHF or wide-band circuits; could be used to provide secure point to point teletype and facsimile transmissions)
- (d) Sorcerer (primarily designed for point to point ciphony over long and short distance circuits of normal band width)

~~TOP SECRET~~

~~TOP SECRET~~

- (e) AN/TRA 16 (primarily designed for microwave point to point radio relay links, carrying 8 voice channels; can handle teleprinter with frequency multiplex)
- (f) D-70 (primarily designed for microwave point to point radio relay links, carrying 12 voice channels; can carry facsimile or teleprinter with frequency multiplex)
- (g) TSS (primarily designed for air-to-air and air-to-ground voice privacy system with minimum security of 20 minutes. Will operate with any existing U.S. aircraft voice transmitter or receiver, on frequencies as low as 175 KCS.)

E. Teleprinter Systems for the exchange of intelligence material.

communications

~~TOP SECRET~~