

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON 25, D.C.

~~TOP SECRET~~
~~SECURITY INFORMATION~~

~~TOP SECRET~~
~~Security Information~~

MEMORANDUM

From: Chief of Naval Operations
To: Joint Chiefs of Staff

Subj: JCS 2074/22; Replacement of the Combined Cipher Machine

Encl: (1) Draft Memorandum

1. The Chief of Naval Operations agrees with the urgency of deciding on a cryptoprinciple to replace the present CCM cryptoprinciple but does not agree with the proposal that ADONIS be recommended to the Representatives of the British Chiefs of Staff as made by the Director, National Security Agency in his Memorandum of 23 December 1952 contained in JCS 2074/22 nor in the Draft Memorandum attached thereto.
2. The Chief of Naval Operations proposes instead to honor existing agreements for the introduction of BRUTUS as the new Combined U. S./ U. K. and NATO cryptoprinciple and recommends substitution of the Draft Memorandum enclosed herewith as the reply to the Representatives of the British Chiefs of Staff.

~~TOP SECRET~~
~~Security Information~~

Declassified and approved for release by NSA on 01-28-2014 pursuant to E.O. 13526

~~TOP SECRET~~

COPY # _____ OF 40 COPIES

~~TOP SECRET~~
~~SECURITY INFORMATION~~

ENCLOSURE

DRAFT

~~TOP SECRET~~
~~Security Information~~MEMORANDUM FOR THE REPRESENTATIVES OF THE BRITISH CHIEFS OF STAFF

Subject: Replacement of the Combined Cipher Machine

1. The United States Joint Chiefs of Staff concur with the views expressed by the United Kingdom Chiefs of Staff in ACT 96, dated 5 December 1952, concerning the adoption of the BRUTUS cryptoprinciple as the new combined U.K./U.S. and NATO cipher system.

2. The United States Joint Chiefs of Staff agree as to the urgency and importance in reaching agreement on this problem. Further delays can be avoided by our making a firm and final decision as to the cryptoprinciple to be employed in the new Combined Cipher Machine. This will then permit our respective technical organizations to take rapid, concerted and simultaneous action to obtain the equipments which embody the agreed principle. Accordingly, in light of the lack of adequate service tests for the POLIUX cryptoprinciple, and the need for a decision at this time based on known facts and proven principles, the U. S. Joint Chiefs of Staff propose that:

a. The cryptoprinciple BRUTUS, as heretofore agreed upon, be designated as the new Combined and NATO cipher system.

b. The United Kingdom and United States jointly prepare a plan for introduction of BRUTUS to begin on 1 January 1955.

c. The U. S. make available to the U. K., under arrangements to be determined later, U. S. BRUTUS equipments required in excess of modified existing machines until such time as the U. K. can provide for its own version of BRUTUS.

d. The incorporation of a pluggable output be investigated and that this highly desirable feature be provided when practicable.

3. It is realized that introduction of BRUTUS will involve adaption of many 10-15 year old machines for the BRUTUS principle. It is, however, envisioned that these equipments will be replaced as rapidly as possible, but that they will:

~~TOP SECRET~~

Enclosure

~~TOP SECRET~~
~~Security Information~~

~~TOP SECRET~~
~~SECURITY INFORMATION~~

~~TOP SECRET~~
~~Security Information~~

- a. Provide a backlog of equipments for NATO use.
 - b. Represent standby equipments for use in the event of hostilities.
4. The U. S. Chiefs of Staff consider the potential reserve value of the CCM (CSP 1700) of sufficient magnitude to embark on a program of modernization of these machines to provide BRUTUS operation. The feasibility of such a modification has been proven (AFSAM 48) and phased conversion will be accomplished as new BRUTUS machines are introduced and CCMs become available.
5. It is therefore urged that you accept the proposals contained herein and that you inform us of your acceptance as quickly as possible.

~~TOP SECRET~~

Enclosure

~~TOP SECRET~~
~~Security Information~~