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

OP-20D/ef
(SC) N36-10
Serial 00736P20

30 January 1948

From: Chief of Naval Communications
TO: Chief, Army Security Agency

Subject: Comments on Army Proposals Regarding the CCM

Reference: (a) Army Security Agency Statement on CCM - Conference with Navy on 1 December 1947

1. It is appreciated that the Army is not in a position to undertake any changes in the present CCM until the SIGROD program has been completed. This, however, should not prevent the two services reaching agreement and firm commitments between themselves as to the future program. It is believed that any new "CCM" must work with the improved ECM (CSP 2900) merely through insertion of the proper basket and rotors, and setting any switching arrangements permanently installed in the basic machine (ECM). This debars too radical departure from the present SIGROD/CSP 1700, or from the present SIGABA/CSP 889. The Navy's rehabilitation and modernization program for the ECM is just beginning and changes can be made now. A year hence the Navy will be too far along in this program to accept alterations. Consequently, an early, coordinated decision as to the future CCM for interim use, as well as for possible long-range use, is considered essential to the national interest.

2. The Navy's Cryptographic Research program prescribed by the Chief of Naval Operations in May 1947 gives top priority to the following three projects:

a. Modernization of existing equipment.

b. Adapting existing equipment to teletype and other rapid means of communication.

c. Improvement of communication security.

Inasmuch as the ASA is prohibited by higher authority from attempting to improve existing equipment, it would appear logical for the Army to accept the Navy's developments along these lines.

3. The proposal for more frequent change of CCM rotors probably is impractical at this time for reasons of expense and lack of reserve rotors in both services. The twice daily change of keylists would be a source of confusion and is therefore considered impracticable.

4. There are five possible programs for the Combined Cipher Machine, namely:

a. Continue with the present system, with which the U. S. Navy and British are dissatisfied. We do not feel that the present CCM has sufficient inherent security for highly important secret messages. The practical effective security of CCM appears to be reducing steadily.

b. Use the Navy's improved "CCM" modifications, including reverse stepping, and possibly with further modifications. The British are using reversed stepping in their RM-26 so this would give the British nothing they do not already know. This is the only program which now appears satisfactory to the Navy.

c. Make the SIGABA/CSP 889 available to the British in event of emergency. It is unacceptable to the Navy to give the ECM to the British at this time or to commit the United States to this action at some future date.

d. Adopt the RM-26 - if, when, and as developed by the British. This will be unacceptable to the Navy for reasons of increased cost, lack of space aboard ship for a second machine, uncertain efficiency of the British machine, and probable long delay in obtaining any workable production models.

e. Adopt the "radically different" machine referred to in reference (a). The Navy cannot agree for two reasons:

(1) No Cryptographic Aid for combined use can be accepted until thoroughly tested and in production, even if not in current use.

(2) The Navy cannot foresee the elimination of Morse Code afloat and in the field and therefore cannot accept any cipher based on a 32-character alphabet or requiring sole use of teletype apparatus.

COPY

5. The Army is again requested to accept CSP 2900 in principle, to undertake this conversion in connection with its own "rehabilitation program," and to agree on a target date for making CSP 2900 effective for Joint Communications."

6. It is believed that the British should be given no further information on these matters until firm Joint understanding and agreement have been reached.

/s/ Ear E. Stone