

SECRET - NATO

COPY NO. 1

NORTH ATLANTIC MILITARY COMMITTEE
COMITE MILITAIRE DE L'ATLANTIQUE NORD

Standing Group

Groupe Permanent

SGM-325-59

REGRADED NATO UNCLASSIFIED

5 June 1959

Per Authority IMSM-431-99

Pages 1-2, Incl.

By JACOUBLE Date 4-1-2000

MEMORANDUM FOR: Allied Commanders-in-Chief, Channel
Military Agency for Standardization
European Communications Security Agency

SUBJECT: Cryptosystem for Minesweeping Communications

- References: a. MAS(NAVY)(57)12 of 18 Mar 57
- b. ECSA Serial 410 of 11 Feb 58
- c. MC 74 (Final Decision)
- d. SGM 120-59

1. At their meeting in Rome in January 1957, the Mine Counter-measures Working Party of the Naval Board of the Military Agency for Standardization (MAS) approved a report of the Working Group (Enclosure 1 to reference a) which agreed that:

- a. The cipher equipment TSEC/KL-7 should be adopted for all minesweepers requiring a high grade cipher system.
- b. A requirement exists in minesweeping communications for a low grade tactical code.

2. The Standing Group supports these requirements and, with regard to the high grade cipher system, the Military Committee in Permanent Session has agreed that the TSEC/KL-7 equipment would satisfy the NATO requirements for cryptographic machine systems for use in inshore and coastal minesweepers. However, it is not possible to determine when such use will become effective NATO-wide (references c and d).

3. The Standing Group does not concur in the requirement expressed in Enclosure I to reference a that a high grade non-mechanical system also is needed. The only available system which

DISTRIBUTION: A D4 E1,2,3,5 H1-4,7-10

SECRET - NATO
SGM-325-59

DECLASSIFIED-PUBLIC DISCLOSURE IMSM-0431-99 DECLASSIFIE-MISE EN LECTURE PUBLIQUE

4/13/78

Page 3

NATO UNCLASSIFIED

APPROVED FOR PUBLIC DISCLOSURE

SECRET - NATO

meets this description is a one-time pad, suggested by France in reference b. It would be exceedingly difficult to organize the distribution of one-time pads so that all ships in a rapidly and ever changing operational pattern would hold the right pad at the right time. The Standing Group considers that installation and use of TSEC/KL-7 in minesweepers should proceed as rapidly as possible. NATEX will remain the primary cipher system until the TSEC/KL-7s are in place, and then will remain as the back-up system.


4. The requirement for a low grade tactical code is supported for use where speed of communication at tactical levels is a major factor.

5. It is understood that CINCHAN, as the NATO command most concerned with minesweeping communications, has done much work on tactical codes. Since it is not considered practicable to adapt either the Maritime and Maritime Aircraft Code (AMSP 258) or the proposed Naval Tactical Code to minesweeping operations, it is requested that CINCHAN submit proposals to the Standing Group for a minesweeping tactical code suitable for NATO-wide operation and for use in conjunction with ATP 19 when that publication is available.

6. The Military Agency for Standardization will be kept informed of action taken.

FOR THE STANDING GROUP:

JHE/md


J. H. EAMAN
Colonel, Canadian Army
Deputy Secretary

SECRET - NATO
SGM-325-59

- 2 -

 UNCLASSIFIED

APPROVED FOR PUBLIC DISCLOSURE

DECLASSIFIED-PUBLIC DISCLOSURE IMSM-0431-99 DECLASSIFIE-MISE EN LECTURE PUBLIQUE