CONFIDENTIAL - NATO COPY NO. 1

NORTH ATLANTIC MILITARY COMMITTEE

COMITE MILITAIRE DE L'ATLANTIQUE NORD 1242

Standing Group Groupe Permanent

SGM-264-56

30 March 1956

MEMORANDUM FOR THE CHAIRMAN, EUROPEAN COMMUNICATIONS SECURITY AGENCY

SUBJECT: Authentication Systems for Use in Exercises

References: a. ECSA Serial 682 of 12 Dec 55
b. ECSA/M10(55), para 26
c. SGM-234-55

1. In reply to paragraph 1 of reference a, AMSP 249 is not intended for use in large-scale exercises, since this edition contains only seven days' key and is considered inadequate for the purpose. This document may be used, as stated in reference c, for day-to-day exercises as well as for classroom training.

2. AMSP 248(I) has been designated as the permanent exercise edition of the Naval and Maritime Air Authentication System, and is to be used for large-scale exercises which do not require security of authentication. (Because of its continual re-use, the authentications derived from AMSP 248(I) must be considered insecure.) Exercise commanders may assign different days' key from this edition for use by opposing forces. Since this edition contains 31 days' key, there should be no necessity for the use of scrambles of the authentication tables, as suggested in sub-paragraph b of reference b. AMSP 248(I) may also be used for day-to-day exercises if desired.

3. In certain special exercises, security of authentication may be required. In such cases the exercise commander should request an unused exercise edition of AMSP 248 from the Standing Group Distribution and Accounting Agency, NATO (DACAN) a sufficient period of time in advance of the exercise to permit distribution. At the

DIST: A1-6,8,10,11,13,16 E1,2,3 H7-9

end of the exercise, the exercise edition used should be destroyed.

4. This information will be disseminated to the Supreme Commanders and Member Nations in a future SGM which will clarify the use of exercise editions of this and other NATO cryptosystems.

FOR THE STANDING GROUP:

C. H. SAMPSON
Commander, USN
Deputy Secretary