

CONFIDENTIAL - NATO

COPY NO. 1

NORTH ATLANTIC MILITARY COMMITTEE

1244

COMITE MILITAIRE DE L'ATLANTIQUE NORD

Standing Group

Groupe Permanent

SGM-235-57

3 April 1957

MEMORANDUM FOR THE CHAIRMAN, EUROPEAN COMMUNICATIONS SECURITY AGENCY

SUBJECT: Encryption of Proforma Type Messages

Reference: ECSA Serial 093 of 20 Dec 56

Frequent use of Category B cryptosystems for encryption of proforma type messages may endanger the security of such systems. The stereotypic characteristics of proforma type messages provide a good basis for cryptanalytic attack. Category B cryptosystems should, therefore, only be used for encryption of proforma type messages when no Category A system is available.

FOR THE STANDING GROUP:

CHS/md

C. H. SAMPSON
Commander, U.S. Navy
Deputy Secretary

311.5

DISTRIBUTION: A E1,2,3 H7

CONFIDENTIAL - NATO
SGM-235-57

CANCELLED

DOCUMENT DESTRUCTION MEMO. #5, 8 Aug 69

DECLASSIFIED-PUBLIC DISCLOSURE IMSM-0001-2006 DECLASSIFIE-MISE EN LECTURE PUBLIQUE