NCSC-5

NATIONAL POLICY
ON
USE OF CRYPTOMATERIAL BY ACTIVITIES OPERATING IN HIGH RISK ENVIRONMENTS (U)

NATIONAL COMMUNICATIONS SECURITY COMMITTEE

NCSC

NATIONAL COMMUNICATIONS SECURITY COMMITTEE

FOREWORD

The National Communications Security Committee approved this policy in January 1981 to replace the policy contained in USCSB 5-7, National Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments, dated 9 September 1970.

This policy provides guidance on the selection and protection of machine cryptosystems for use in high risk environments by the Heads of Federal Departments and Agencies, the Joint Chiefs of Staff, the Commanders of the Unified and Specified Commands and Military Commanders. The Director, National Security Agency, shall in coordination with the other members of the NCSC, establish standardized criteria for the identification of high risk environments, as well as establish and publish the criteria for the selection of the appropriate machine cryptosystems. These implementing guidelines, previously included as an appendix to USCSB 5—7, will be promulgated by appropriate National COMSEC Instructions.

FOR THE EXECUTIVE AGENT FOR COMMUNICATIONS SECURITY:

NATIONAL POLICY
ON
THE SELECTION AND PROTECTION OF
MACHINE CRYPTOSYSTEMS FOR USE IN HIGH RISK
ENVIRONMENTS

6 January 1981

Section 1—Policy

1. It is the policy of the United States Government that:

a. The selection of machine cryptosystems for use in high risk environments shall be a deliberate decision taking into consideration the factors promulgated by the Director, NSA. High risk environments for machine cryptosystems shall be identified in accordance with standardized criteria.

b. In all cases where machine cryptosystems will be used in high risk environments a workable plan will be developed and implemented to protect, evacuate, or destroy COMEC equipment and other COMSEC materials which may be jeopardized.

c. Only the minimum amount of mission essential COMSEC material may be located at high risk environments.

d. Point-to-point keying material, rather than netted or common user keying material, will be used for secure communications to high risk areas.

Section II—Responsibilities

2. The Heads of Federal Departments and Agencies, the Joint Chiefs of Staff, the Commanders of the Unified and Specified Commands, and Military Commanders are responsible for:

a. Identifying specific high risk locations where machine cryptosystems may be deployed in accordance with standardized criteria, and notifying the Director, NSA, of all such designations.

b. Applying the criteria published by the Director, NSA, in the selection of machine cryptosystems for use in high risk environments and notifying the Director, NSA, of their selection.

c. Selecting, procuring, installing, operating, and maintaining machine cryptosystems selected for use in high risk environments.

d. Assuring that only minimum amounts of mission essential COMSEC materials are placed in high risk environments.

e. Assuring that effective and workable plans, and adequate manpower and materials are available to protect, evacuate, or destroy COMSEC materials in high risk locations which are jeopardized.

f. Notifying appropriate COMSEC authorities when machine cryptosystems used in high risk environments are destroyed, lost, damaged, captured or compromised.

g. Making reasonable efforts to return abandoned equipments and COMSEC materials to proper control.

3. The Director, NSA, is responsible for:

a. Coordinating with the other members of the NCSC in establishing standardized criteria for the identification of high risk environments.

b. Establishing and publishing the criteria for the selection of machine cryptosystems intended for use In high risk environments.

c. Maintaining overnight regarding the selection of machine cryptosystems for use in a high risk environment and notifying appropriate officials when, in his judgement, an inappropriate choice has been made.

Section III—Exceptions

4. Operations covered by NSCID No. 5; ships, aircraft and ground units on hazardous or nuclear safety related missions; and operations which are time-sensitive or conducted during active combat, are exempt from the advance reporting requirements of paragraph 2*a* and 2*b* of this policy.