CNSS Policy No.1
September 2004

NATIONAL POLICY
FOR
SAFEGUARDING AND CONTROL OF
COMSEC MATERIALS

Committee on National Security Systems

FOREWORD

1. As part of an ongoing effort to ensure that CNSS issuances are relevant and current, the Policy Review and Compliance Working Group reviewed NCSC-1 and determined that significant changes were not required. This policy is being issued to revalidate and renumber NCSC-1, National Policy for Safeguarding and Control of Communications Security Materials, dated 16 January 1981. It establishes a system for the control of communications security (COMSEC) material within the U.S. Executive Departments and Agencies.

2. Representatives of the Committee on National Security Systems may obtain additional copies of this Instruction at the address listed below.

3. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

/s/

LINTON WELLS II
Chair

CNSS Secretariat (I01C) . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL POLICY FOR SAFEGUARDING AND CONTROL OF COMSEC MATERIALS

SECTION

SECTION I – SCOPE AND APPLICABILITY

1. The provisions of this policy are applicable to all U.S. Government Departments and Agencies authorized access to, or custody of, COMSEC materials or techniques.

2. The term COMSEC material as used in this policy includes any information in physical form whose intended purpose is to deny unauthorized persons information derived from telecommunications of the United States Government related to national security, or to ensure the authenticity of such communications. It includes, but is not limited to: (a) COMSEC keying material in any form to protect or authenticate national security or national security-related information, which must be transmitted, communicated, or processed by electrical, electromagnetic, electromechanical, or electro-optical means; (b) those items which embody, describe, or implement a cryptographic logic; and (c) other items produced by or for the U.S. Government for communications security purposes.

SECTION II – POLICY

3. It is the policy of the United States Government to safeguard and control COMSEC materials in a manner which assures their continued integrity, prevents access by unauthorized persons and controls the spread of COMSEC materials, techniques, and technology when not in the best interest of the United States and its Allies.

4. In furtherance of this policy, there shall be established within each Department and Agency holding COMSEC keying material a COMSEC Material Control System, into which all COMSEC keying material will be placed. Other COMSEC material may be placed in the COMSEC Material Control System or any other material control system, which provides the requisite degree of security, accounting, modification, and management control.

SECTION III - RESPONSIBILITIES

5. The Heads of Departments and Agencies are responsible for implementing within their Department or Agency the provisions of this policy.

6. The Director, National Security Agency shall:

a. Prescribe the minimum-security standards for performance of Central Office of Record Functions by the Federal Departments and Agencies.
b. Collaborate with the Departments and Agencies to:

(1) Establish procedures for reporting and evaluating communications security weaknesses; and
(2) Establish doctrine and procedures to protect communications security information.

c. Authorize, on a case-by-case basis, exceptions to compliance with the standards contained in CNSS Instructions concerning the safeguarding and control of COMSEC information and performance of COMSEC Material Central Office of Record functions.

SECTION IV – EXCEPTIONS

7. The Central Intelligence Agency in the performance of functions described by NSCID No. 5 is specifically exempted from this policy.