CNSS Policy No. 6
October 2005

NATIONAL POLICY
ON
CERTIFICATION AND ACCREDITATION
OF
NATIONAL SECURITY SYSTEMS

CNSS Policy No. 6

Committee on National Security Systems

FOREWORD

1. The national security community, in order to ensure the security of National Security Systems, is developing cost-effective policies, procedures, and methodologies for the certification and accreditation (C&A) of national telecommunications and information systems. This C&A policy for National Security Systems will begin to provide the community with standard methodologies for C&A processes, assign authority and responsibilities, and lay a basis for mutual recognition of certification results. This policy supersedes NSTISSP Policy No. 6, "National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems," dated 8 April 1994.

2. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this policy at the address below.

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

/s/
Linton Wells II

(410) 854-6805 . UFAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL POLICY
ON
CERTIFICATION AND ACCREDITATION OF NATIONAL SECURITY SYSTEMS

SECTION I - POLICY

1. All federal government departments and agencies shall establish and implement programs that mandate the certification and accreditation (C&A) of National Security Systems (NSS) under their operational control. These C&A programs shall ensure that information collected, generated, processed, stored, displayed, transmitted or received by NSS is adequately protected with respect to requirements for confidentiality, integrity, and availability. NTISSI No. 1000, "National Information Assurance Certification and Accreditation Process (NIACAP)" was developed to provide minimum standards for the certification and accreditation of national security systems. Federal departments and agencies shall refer to the NIACAP, or a C&A process that is consistent with the NIACAP, when developing their C&A programs.

2. Nothing in this policy alters or supersedes the existing authorities of the Director of National Intelligence.

SECTION II - DEFINITIONS

3. The following definitions were taken from CNSSI No. 4009, National Information Assurance (IA) Glossary unless otherwise noted.

a. Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (C&A Working Group definition.)

b. Certification - Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

c. Designated Approving Authority (DAA) - Official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

d. Information System (IS) - Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

e. National Security System (NSS) - Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency,

(1) the function, operation, or use of which:

involves intelligence activities;

involves cryptologic activities related to national security;

involves command and control of military forces;

involves equipment that is an integral part of a weapon or weapon system; or

(subject to Subparagraph (B)*) is critical to the direct fulfillment of military or intelligence missions; or

(2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

*Subparagraph B – Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 44 U.S.C. 3542, Federal Information Security Management Act of 2002)

f. Telecommunications - Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

SECTION III - PRINCIPLES

4. C&A programs established to satisfy this policy shall be based on the following principles:

a. Certification of NSS shall be performed and documented in accordance with specified criteria, standards, and guidelines.

b. All NSS shall be accredited by DAAs. The DAA shall be in a position to balance operational mission requirements and the residual risk of system operations, and to understand the risk of accepting interconnection to other systems and networks outside of the DAA's authority. All accreditation decisions shall be documented and contain a statement of residual risk.

c. Departments and agencies shall freely exchange technical C&A information, coordinate programs, and participate in cooperative projects wherever possible consistent with the classification and sensitivity of the C&A information and results.

d. To promote cost-effective security across the federal government, department and agency programs for the C&A of NSS shall be developed in concert with similar programs that address the security of non-NSS.

e. As cornerstones of a continuous process of effective security management, activities in support of C&A shall be performed throughout the total system life cycle.

SECTION IV - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall:

a. ensure their C&A program is consistent with the policy and principles set forth in this CNSS policy,

b. ensure that a DAA is appointed for each system under their operational control and

c. ensure that the appointed DAA is aware of his or her responsibilities as outlined in CNSSI No. 4012, " National Information Assurance Training Standard for Senior System Managers."

6. The National Manager for the CNSS, in coordination with CNSS members and others as appropriate, shall develop and promulgate minimum technical criteria, standards, and guidelines for the certification and accreditation of NSS.