NSTISSP No. 6

8 April 1994

NATIONAL POLICY

ON

CERTIFICATION AND ACCREDITATION OF

NATIONAL SECURITY TELECOMMUN1CATIONS

AND INFORMATION SYSTEMS

FOREWARD

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 national certification and accreditation policy 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.

EMMETT PAIGE, JR.

NATIONAL POLICY
ON
CERTIFICATION AND ACCREDITATION OF NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION 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 under their operational control. These C&A programs shall ensure that information processed, stored, or transmitted by national security systems is adequately protected with respect to requirements for confidentiality, integrity, and availability.

SECTION II - DEFINITIONS

2. Accreditation - Formal declaration by a Designated Approving Authority (DAA) that a system* is approved to operate in a particular security mode using a prescribed set of safeguards.

3. Certification - Comprehensive evaluation of the technical and nontechnical security features of a system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

4. Designated Approving Authority - Official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk.

5. National Security Systems - Telecommunications and automated information systems operated by the U.S. Government, its contractors, or its agents, that contain classified information or, as set forth in 10 U.S.C. Section 2315, that 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 involves equipment that is critical to the direct fulfillment of military or intelligence missions.

---

*. The official definitions in NSTISSI 4009 uses the term “AIS” rather than “system.” For the purposes of this policy, however, the terms “AIS” and “AIS or network” are defined to be synonymous with “national security system” (commonly abbreviated as “system.”)

SECTION III - PRINCIPLES

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

a. Certification of national security systems shall be performed and documented by competent personnel in accordance with specified criteria, standards, and guidelines.

b. Accreditation of national security systems shall be performed by competent management personnel in a position to balance operational mission requirements and the residual risk of system operation. 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.

d. To promote cost-effective security across the federal government, department and agency programs for the C&A of national security systems shall be developed in concert with similar programs that address security of sensitive information pursuant to the Computer Security Act of 1987 (Public Law 100-235)

e. As cornerstones of a continuous process of effective security management, activities in support of certification and accreditation shall be performed at appropriate points throughout the total system life cycle.

SECTION IV - RESPONSIBILITIES

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

a. ensure that C&A programs consistent with the policy and principles set forth in this NSTISSP are established and implemented, and

b. ensure that a DAA is identified for each system under their operational control, and that DAAS have the ability to influence the application of resources to achieve an acceptable level of security.

8. The National Manager for National Security Telecommunications and Information Systems Security, in cooperation with the members of the National Telecommunications and Information Systems Security Committee (NSTISSC) and others as appropriate, shall develop and promulgate technical criteria, standards, and guidelines for the certification of national security systems.

DISTRIBUTION:

EXEC (REG)
C/S
AGC/I
ADIL
GC
BO3
C/SCI (2)
C
C6
C7
C9
F1A
F1C
FlD
FlE
F1F
F1G
ElH
F1I
F1L
F1M
F2 (5)
F32
F321
F33
F34
F38
F4 (5)
F41
F45
F47
F6
F81
F83
F91
F92
F92 (Vital Records)
G
I
I2
Il
Il/S
Ill
I9

J
J C/S
J06
J3
K
K509
K5ll
L06
M509
M51
M52
NSALO/DISA
N5
N51
N52
P
P04
P1
P6
Q3
R
R2
R23
R7
RB
T09
V
V2 (9)
V23
V4
V49 (5)
V6
V7
V8
X
X8
X81
X813
X82
X821
X822
X823
X84
X6

Y
Y1
Y106
Yl3 (6)
Y134
Y2(21)
NSTISSC Secretariat (5O)