CNSS Directive No. 502
16 December 2004

National Directive
On
Security of National Security Systems

Committee on National Security Systems

Chair

FOREWORD

1. National Security Directive (NSD)-42, "National Policy for the Security of National Security Telecommunications and Information Systems," signed by the President on July 5, 1990, established initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding from exploitation, systems that process or communicate national security information; established a mechanism for policy development; and assigned responsibilities for implementation. This directive clarifies objectives, policies, procedures, standards, and terminology as set forth in the national policy as well as follow up executive orders, amendments, and changes.

2. This document updates and supercedes NSTISSD No. 502, dated 5 February 1993.

3. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this directive from the CNSS web site (www.cnss.gov) or by contacting the Secretariat at the address below. U.S. Government contractors are to contact their appropriate government agency Contracting Officer Representative regarding distribution of this document.

/s/
Linton Wells II

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 DIRECTIVE
ON
SECURITY OF NATIONAL SECURITY SYSTEMS

SECTION I - PURPOSE

1. This directive delineates and clarifies objectives, policies, procedures, standards and terminologies as set forth in the "National Policy for the Security of National Security Telecommunications and Information Systems, (NSD-42)" dated July 5, 1990 (hereinafter referred to as "the national policy"). National Security Directive (NSD)-42 establishes initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from hostile exploitation, systems which process or communicate national security information; establishes a mechanism for policy development; and assigns responsibilities for implementation. NSD-42 establishes an interagency group at the operating level, an Executive Agent, and a National Manager to implement these objectives and policies. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of NSD-42. On October 16, 2001, the President signed Executive Order 13231, Critical Infrastructure Protection in the Information Age, redesignating the NSTISSC as the Committee on National Security Systems (CNSS). The Department of Defense continues to chair the CNSS under the authorities established by NSD-42. This was reaffirmed by Executive Order 13284, dated January 23, 2003, Executive Order Amendment of Executive Orders and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security.

SECTION II - APPLICABILITY AND SCOPE

2. This Directive applies to all Executive departments, agencies, and U.S. Government contractors who own, procure, use, operate, or maintain national security systems as defined by this directive.

3. This Directive does not apply to those systems that directly or indirectly operate under the authority of the DCI (all systems processing intelligence information (SCI), intelligence

related Special Access Programs (SAPs), and Sources and Methods information (SAMI) related distribution.

SECTION III - OBJECTIVES

4. Ensuring the security of national security systems is vitally important to the operational effectiveness of the national security activities of the government and to military combat readiness. Therefore, the national policy directed that the government's capabilities for securing national security systems against technical exploitation threats be maintained or, if inadequate, improved to provide for:

a. Reliable and continuing assessment of threats and vulnerabilities, and implementation of appropriate, effective countermeasures;

b. A technical base within the U.S. Government to achieve this security, and initiatives with the private sector to maintain, complement, or enhance that government technical base and to ensure information assurance products are available to secure national security systems; and,

c. Effective and efficient application of U.S Government resources.

SECTION IV - POLICIES

5. In support of these objectives, the following policies were established:

a. U.S. Government national security systems shall be secured by such means as are necessary to prevent compromise, denial, or exploitation;

b. Federal agencies shall require that national security systems operated and maintained by U.S. Government contractors likewise be secured.

SECTION V - RESPONSIBILITIES

6. The Committee on National Security Systems

a. The CNSS was established to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement provisions of the national policy. The Committee is chaired by the Assistant Secretary of Defense Networks and Information Integration/Chief Information Officer (ASD/NII/CIO) and is composed of a voting representative of each of the following:

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Attorney General
The Secretary of Commerce

The Secretary of Homeland Security
The Secretary of Transportation
The Secretary of Energy
Director, Office of Management and Budget
Assistant to the President for National Security Affairs
Director of Central Intelligence
Chairman of the Joint Chiefs of Staff
Director, Federal Bureau of Investigation
Administrator, General Services Administration
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, National Security Agency
Director, Defense Intelligence Agency

b. The CNSS:

1) Develops such specific operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as may be required to implement the national policy;

2) Provides systems security guidance for national security systems to Executive departments and agencies;

3) Submits, as consistent with requirements satisfied by Ref f, to the Executive Agent an evaluation of the security status of national security systems with respect to established objectives and priorities;

4) Approves the release of Information Assurance material, information, and techniques to foreign governments or international organizations. The concurrence of the Director of Central Intelligence is obtained with respect to those activities which he manages;

5) Establishes and maintains a national system for promulgating the operating policies, instructions, directives, and guidance, which may be issued pursuant to the national policy;

(6) Establishes permanent and temporary subcommittees as necessary to discharge its responsibilities;

(7) Makes recommendations on membership and establishes criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

c. The Committee has two subcommittees, one focusing on telecommunications security and one focusing on information systems security. The two subcommittees coordinate

their actions and recommendations concerning implementation of protective measures, and combine where appropriate.

d. The Committee has a permanent secretariat composed of personnel of the National Security Agency and such other personnel from Executive departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency provides facilities and support as required. Other Executive departments and agencies provide facilities and support as requested by the Chairman.

7. The Executive Agent of the Government for National Security Systems.

a. Consistent with the authority for communications security given the Secretary of Defense in Executive Order 12333, the Secretary of Defense serves as Executive Agent of the Government for National Security Systems and is responsible for implementing, under his signature, policies and procedures to:

1) In conjunction with Committee member departments and agencies, ensure the development of plans and programs to fulfill the objectives of this directive, including the development of necessary security architectures;

2) Procure for and provide to Executive departments and agencies and, where appropriate, to government contractors and foreign governments, consistent with the laws of the United States, such technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of the national policy;

3) Approve and provide minimum security standards and doctrine for systems subject to the national policy;

4) Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems; and,

5) Operate or coordinate the efforts of U.S. Government technical centers related to national security systems.

b. The Executive Agent reviews and assesses the National Manager's recommendations on the proposed national security systems programs and budgets for the Executive departments and agencies. Where appropriate, alternative systems security recommendations are provided to agency heads, to National Security Council Committees, and to the OMB. Consistent with ANNEX A, Ref. f, the Executive Agent submits the security status of national security systems with respect to established objectives and priorities through the National Security Council to the President.

8. The National Manager for National Security Systems - The Director, National Security Agency, was designated the National Manager for National Security Systems and is

responsible to the Secretary of Defense, Executive Agent, for carrying out the foregoing responsibilities. In fulfilling these responsibilities, the National Manager:

a. Examines U.S. Government national security systems and evaluates their vulnerability to foreign interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, are conducted in strict compliance with law; Executive Order and implementing procedures; the national policy; and applicable Presidential directive. No monitoring is performed without advising the heads of the agencies, departments, or Services concerned;

b. Acts as the U.S. Government focal point for Information Assurance for national security systems;

c. Conducts, approves, or endorses research and development of techniques and equipment to secure national security systems;

d. Reviews and approves all information assurance security standards, techniques, systems, and equipment related to the security of national security systems;

e. Conducts foreign information assurance liaison, including entering into agreements with foreign governments and with international and private organizations regarding national security systems, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Any such agreements shall be coordinated with affected departments and agencies and in accordance with NSTISSP No. 8;

f. Operates such printing and fabrication facilities as may be required to perform critical functions related to the provisions of cryptographic and other technical security material or services;

g. Assesses and disseminates information on the overall security posture of threats to and vulnerabilities of national security systems;

h. Operates a central technical center to evaluate and certify the security of national security systems;

i. Prescribes the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information related to national security systems;

j. Reviews and assesses, consistent with ANNEX A, Ref.f, the national security systems programs and budgets of Executive departments and agencies of the U.S. Government, and recommends alternatives, where appropriate, for the Executive Agent;

k. Reviews, consistent with ANNEX A, Ref. f, the aggregated national security systems program and budget recommendations of the Executive departments and agencies of the U.S. Government for the Executive Agent;

l. Requests from the heads of Executive departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein;

m. Coordinates with the National Institute for Standards and Technology in accordance with the provisions of the Computer Security Act of 1987 (P.L. 100-235) and,

n. Enters into agreements for the procurement of technical security material and other equipment, and their provision to Executive departments and agencies, where appropriate, to government contractors, and foreign governments.

9. The Heads of Executive Departments and Agencies are responsible for:

a. Achieving and maintaining secure national security systems within their departments or agencies;

b. Ensuring that policies, procedures, guidelines, instructions, and standards issued pursuant to the national policy are implemented within their departments or agencies; and,

c. Providing to the CNSS, the Executive Agent, and the National Manager, as appropriate, such information as may be required to produce assessments of the status of national security systems as consistent with ANNEX A, Ref. f, or to fulfill responsibilities assigned herein, consistent with relevant law, Executive Order, the national policy and Presidential directive.

10. The Director, Office of Management and Budget, is responsible for:

a. Specifying data to be provided during the annual budget review by Executive departments and agencies (ANNEX A, Ref. f) on program and budgets relating to security of national security systems;

b. Consolidating and providing such data to the National Manager via the Executive Agent; and,

c. Reviewing for consistency with the national policy, and amending as appropriate, OMB policies and regulations that may pertain to the subject matter herein.

SECTION VI - EXCLUSIONS

11. Nothing in this Directive

a. Alters or supersedes the existing authorities of the Director of Central Intelligence:

b. Authorizes the Committee, the Executive Agent, or the National Manager authority to examine the facilities of other Executive departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein;

c. Amends or contravenes the provisions of existing law, Executive Order, national policy or Presidential directive which pertain to the protection of sensitive information, to the protection of national security information, to the privacy aspects or financial management of information systems, or to the administrative requirements for safeguarding such resources against fraud, waste, and abuse;

d. Provides authority to issue policies, procedures, guidelines, instructions, standards, or priorities or operate programs concerning security of systems other than national security systems;

e. Is intended to establish additional review processes for the procurement of information processing systems; or

f. Alters or rescinds policies or programs begun under PD-24, NSDD-145, and the national policy, that may be pertinent to national security systems. Policies or programs retained pursuant to this provision shall not be construed to apply to systems within the purview of the Computer Security Act of 1987 (P.L. 100-235).

Encl: ANNEX A

ANNEX A

References

(U) The following references are applicable to this directive:

a. (U) NSD-42, National Policy for the Security of National Security Telecommunications and Information Systems, July 5, 1990.

b. (U) Executive Order 13231, Critical Infrastructure Protection, October 16, 2001, as amended by E.O.s 13284, 13286, 13316.

c. (U) Executive Order 13284, Amendment of EO, and Other Actions, in connection with the Establishment of the Department of Homeland Security, January 23, 2003.

d. (U) P.L. 107-347, E-Government Act, December 2002 (FISMA).

e. (U) Executive Order 12333, United States Intelligence Activities, December 4, 1981, as amended by E.O. 13284.

f. (U) NSTISSP No. 8, National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Foreign Government, 13 Feb 97.

g. (U) Public Law 100-235, Computer Security Act of 1987, January 8, 1988.

h. (U) PD-24, Telecommunicatons Protection Policy, November 16, 1977.

i. (U) NSDD-145, National Policy on Telecommunications and Automated Information Systems Security, September 17, 1984.

j. (U) Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Function April 3, 1984, as amended by E.O. 13286.

k. (U) Executive Order 12958, Classified National Security Information, April 2, 1982, as amended by E.O.s 12972, 13142, 13292.

l. (U) Information Technology Management Reform Act of 1996 (Div. E of P.L. 104-106) (Clinger-Cohen Act).

m. (U) CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003.

n. (U) NSTISSD No. 900, Governing Procedures of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), April 2000.

o. (U) NSTISSD No. 901, National Telecommunications and Information Systems Security Issuance System, April 2000.