~~CONFIDENTIAL~~ UNCLASSIFIED 20779 ADD-ON

THE WHITE HOUSE

WASHINGTON

July 5, 1990

NATIONAL SECURITY DIRECTIVE 42

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
DIRECTOR OF THE 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 OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE FEDERAL EMERGENCY MANAGEMENT AGENCY
ADMINISTRATOR OF GENERAL SERVICES
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 OF THE NATIONAL SECURITY AGENCY
MANAGER OF THE NATIONAL COMMUNICATIONS SYSTEM
DIRECTOR, DEFENSE INTELLIGENCE AGENCY

SUBJECT: National Policy for the Security of National Security Telecommunications and Information Systems (U)

Continuing advances in microelectronics technology have stimulated an unprecedented growth in the demand for and supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. (U)

~~CONFIDENTIAL~~
Declassify on: OADR

UNCLASSIFIED

Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. A comprehensive and coordinated approach must be taken to protect the government's national security telecommunications and information systems (national security systems) against current and projected threats. This approach must include mechanisms for formulating policy, overseeing systems security resources programs, and coordinating and executing technical activities. (U)

This Directive establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. It is intended to ensure full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, and to promote a coherent and coordinated defense against the foreign intelligence threat to these systems. This Directive recognizes the special requirements for protection of intelligence sources and methods. (U)

1. Objectives. 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. I, therefore, direct 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; (U)

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 systems security products are available to secure national security systems; and, (U)

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

2. Policies. In support of these objectives, the following policies are established:

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

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

3. Implementation. This Directive establishes an NSC Policy Coordinating Committee for National Security Telecommunications and Information Systems, an interagency group at the operating level, an executive agent and a national manager to implement these objectives and policies. (U)

4. National Security Council/Policy Coordinating Committee for National Security Telecommunications and Information Systems.

The National Security Council/Policy Coordinating Committee (PCC) for National Security Telecommunications, chaired by the Department of Defense, under the authority of National Security Directives 1 and 10, assumed the responsibility for the National Security Telecommunications NSDD 97 Steering Group. By authority of this Directive, the PCC for National Security Telecommunications is renamed the PCC for National Security Telecommunications and Information Systems, and shall expand its authority to include the responsibilities to protect the government's national security telecommunications and information systems. When addressing issues concerning the security of national security telecommunications and information systems, the membership of the PCC shall be expanded to include representatives of the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Energy, the Secretary of Commerce, and the Director of Central Intelligence. The National Manager for National Security Telecommunications and Information Systems Security shall be invited as an observer. The Policy Coordinating Committee shall:

a. Oversee the implementation of this Directive; (U)

b. Develop policy recommendations and provide guidance to the operating level National Security Telecommunications and Information Systems Security Committee (NSTISSC); (U)

c. Review and resolve matters referred to it by the NSTISSC in fulfilling the responsibilities outlined in paragraph 5, below; (U)

d. Be subject to the policies of the Director of Central Intelligence on matters pertaining to the protection of intelligence sources and methods; and, (U)

e. Recommend for Presidential approval additions or revisions to this Directive as national interests may require. (U)

5. The National Security Telecommunications and Information Systems Security Committee.

a. The NSTISSC is established to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be 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 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
Director, Federal Emergency Management Agency
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
Manager, National Communications System
Director, Defense Intelligence Agency (U)

b. The NSTISSC shall:

(1) Develop such specific operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as may be required to implement this Directive; (U)

(2) Provide systems security guidance for national security systems to Executive departments and agencies; (U)

(3) Submit annually to the Executive Agent an evaluation of the security status of national security systems with respect to established objectives and priorities; (U)

(4) Approve the release of cryptologic national security systems technical security material, information, and techniques to foreign governments or international organizations. The concurrence of the Director of Central Intelligence shall be obtained with respect to those activities which he manages; (U)

(5) Establish and maintain a national system for promulgating the operating policies, instructions, directives, and guidance, which may be issued pursuant to this Directive; (U)

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

(7) Make recommendations to the PCC for NSTISSC membership and establish 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; and, (U)

(8) Interact, as necessary, with the National Communications System Committee of Principals established by Executive Order 12472 to ensure the coordinated execution of assigned responsibilities. (U)

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on information systems security. The two subcommittees shall coordinate their actions and recommendations concerning implementation of protective measures, which shall combine and coordinate both areas where appropriate. (U)

d. The Committee shall have 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 shall provide facilities and support as required. Other Executive departments and agencies shall provide facilities and support as requested by the Chairman. (U)

6. The Executive Agent of the Government for National Security Telecommunications and Information Systems Security.

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

(1) Ensure the development, in conjunction with Committee member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures; (U)

(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 this Directive; (U)

(3) Approve and provide minimum security standards and doctrine for systems subject to this Directive; (U)

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

(5) Operate, or coordinate the efforts, of U.S. Government technical centers related to national security telecommunications and information systems security. (U)

b. The Executive Agent shall review and assess the National Manager's recommendations on the proposed national security telecommunications and information systems security programs and budgets for the Executive departments and agencies. Where appropriate,

alternative systems security recommendations will be provided to agency heads, to National Security Council Committees, and to the OMB. In addition, the Executive Agent shall submit, annually, the security status of national security systems with respect to established objectives and priorities through the National Security Council to the President. (U)

7. The National Manager for National Security Telecommunications and Information Systems Security.

The Director, National Security Agency, is designated the National Manager for National Security Telecommunications and Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall:

a. Examine U.S. Government national security systems and evaluate their vulnerability to foreign interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Order and implementing procedures, and applicable Presidential directive. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned; (U)

b. Act as the U.S. Government focal point for cryptography, telecommunications systems security, and information systems security for national security systems; (U)

c. Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems; (U)

d. Review and approve all standards, techniques, systems, and equipment related to the security of national security systems; (U)

e. Conduct foreign computer security and communications security 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; (U)

f. Operate 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; (U)

g. Assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems; (U)

h. Operate a central technical center to evaluate and certify the security of national security telecommunications and information systems; (U)

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

j. Review and assess annually the national security telecommunications systems security programs and budgets of Executive departments and agencies of the U.S. Government, and recommend alternatives, where appropriate, for the Executive Agent; (U)

k. Review annually the aggregated national security information systems security program and budget recommendations of the Executive departments and agencies of the U.S. Government for the Executive Agent; (U)

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

m. Coordinate 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 (U)

n. Enter 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. (U)

8. The Heads of Executive Departments and Agencies shall:

a. Be responsible for achieving and maintaining secure national security systems within their departments or agencies; (U)

b. Ensure that policies, procedures, guidelines, instructions, and standards issued pursuant to this Directive are implemented within their departments or agencies; and (U)

c. Provide to the NSTISSC, the Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential directive. (U)

9. Additional Responsibilities. The Director, Office of Management and Budget, shall:

a. Specify data to be provided during the annual budget review by Executive departments and agencies on program and budgets relating to security of their national security systems; (U)

b. Consolidate and provide such data to the National Manager via the Executive Agent; and (U)

c. Review for consistency with this Directive, and amend as appropriate, OMB policies and regulations which may pertain to the subject matter herein. (U)

10. Nothing in this Directive shall:

a. Alter or supersede the existing authorities of the Director of Central Intelligence; (U)

b. Authorize 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; (U)

c. Amend or contravene the provisions of existing law, Executive Order, 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; (U)

d. Provide authority to issue policies, procedure, guidelines, instructions, standards, or priorities or operate programs concerning security of systems other than national security systems; (U)

e. Be intended to establish additional review processes for the procurement of information processing systems; (U)

f. Alter or rescind policies or programs begun under PD-24 or NSDD-145 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 (PL100-235); or (U)

1.5(d)

[redacted] (C)

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means; (U)

b. Information Systems means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware; (U)

c. Telecommunications and Information Systems Security means protection afforded to telecommunications and information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information; (U)

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and information systems; (U)

e. National security systems are those telecommunications and information systems operated by the U.S. Government, its contractors, or 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. (U)

12. Except for ongoing telecommunications protection activities mandated by and pursuant to PD-24 and NSDD-145, NSDD-145 is hereby rescinded. (U)