Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

CONFIDENTIAL DRAFT

90078

THE WHITE HOUSE

WASHINGTON

CONFIDENTIAL

National Security Decision
Directive Number

NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the demand for telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, electronic penetration, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. (C)

These systems process and communicate classified national security information, other sensitive information concerning vital interests of the United States, and the private or proprietary information of US persons and businesses. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its interests. A comprehensive and coordinated approach must be taken to protect the Nation's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. (C)

This Directive provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed towards safeguarding systems which process or communicate sensitive information, establishes a mechanism for policy development and assigns responsibilities for implementation. The structure proposed in this draft seeks to assure full participation and cooperation among the various

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

COPY 9 OF 9 COPIES

CONFIDENTIAL

Declassify on: OADR

CONFIDENTIAL

DRAFT
Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat, and to foster an appropriate partnership between government and the private sector in attaining these goals. It specifically recognizes the special requirement for protection of intelligence sources and methods. It is intended that the machinery established by this NSDD will initially focus on those automated systems which are connected to telecommunications transmission systems. (C)

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, other sensitive government information, and certain private sector information is a key national responsibility. I, therefore, direct that the Nation's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government and private resources.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems. (U)

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

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secure or protected by such means as are necessary to prevent compromise and exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national interest or the rights of US persons, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national interest.

COPY 9 OF 9 COPIES
Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2
CIA

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

c. The government shall work with the private sector to identify systems which handle sensitive non-government information, the loss of which could adversely affect the national interest or the rights of US persons; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national interest, the private sector shall be encouraged and assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall continue. (U)

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies. (U)

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and National Manager with respect to the activities undertaken by them in implementing this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those national telecommunications and automated information systems that handle classified or sensitive information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review and approve consolidated resources program and budget proposals, and other matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

COPY 9 OF 9 COPIES

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

(5) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(6) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

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

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group. (U)

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by a representative of the Secretary of Defense and shall be composed of a non-voting representative of each member of the Steering Group and a voting representative of each of the following:

The Secretary of State
The Secretary of the Treasury
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
The Director of Central Intelligence
Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
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 (U)

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

(2) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(3) Approve the release of sensitive systems security information, techniques and materials to foreign governments or international organizations (except in intelligence activities managed by the Director of Central Intelligence).

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

(5) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(6) Make recommendations to the Steering Group on Committee 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. (U)

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate while considering any differences in the level of maturity of the technologies to support such implementations. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important. (U)

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from 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 departments and agencies shall provide facilities and support as requested by the Chairman. (U)

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

a. Ensure the development, in conjunction with the National Manager and with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the formulation of necessary security architectures.

b. Fulfill requirements of the government for technical security material and related services.

c. Approve and provide minimum security standards and doctrine.

d. Conduct, approve, or endorse research and development of security techniques and equipment.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Procure for and provide to government agencies, and, where appropriate, to private institutions (including government contractors) and foreign governments, equipment and other materials as required to accomplish the objectives of this Directive.

g. Develop and submit to the Steering Group a proposed National Telecommunications and Information Systems Security Program budget for each fiscal year, including funds for the procurement and provision of equipment and materials. (U)

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

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives.

b. Act as the government focal point for all matters concerning cryptography, communications security, and the security of automated information systems. Responsibilities for protecting sensitive national security related government or government-derived information shall include conducting, approving, or endorsing all research and development of security means; reviewing and approving all standards, techniques, systems and equipments for security protection; and conducting liaison, including agreements, with foreign governments,

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

international and private organizations, for security protection means.

c. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other sensitive technical security materials or services.

d. Operate a central technical center to assess and disseminate information on hostile threats to national telecommunications and automated information systems security and to assess the overall security posture.

e. Operate a central technical center to evaluate and certify the security of telecommunications systems, and automated information systems, and to conduct or sponsor research and development of security techniques.

f. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

g. Review annually the systems security program and resources requirements of the departments and agencies of the government, and prepare consolidated National Telecommunications and Automated Information Systems Security program budget recommendations.

h. Request from the heads of departments and agencies such information and technical support as he may need to discharge the responsibilities assigned herein.

i. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations (including government contractors) and foreign governments. (U)

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining an acceptable security posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, the Secretary of Defense as Executive Agent, and the Director, National Security Agency as National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives. (U)

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Director, National Security Agency may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems, as the Director, National Security Agency may approve. Such standards, while legally applicable only to Federal Departments and Agencies, will be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget shall review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein. (U)

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for purposes not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems. (U)

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

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

DRAFT

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

information by electrical, electromagnetic, electromechnical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated 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 sensitive technical security material and the protection of sensitive technical security information.

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 automated information processing systems. (U)

12. The Interagency Committee on Foreign Real Estate Acquisitions (ICREA) in the United States established under PD-24 shall be reconstituted under the chairmanship of the Director, Office of Foreign Missions, Department of State, with representation from the Department of Defense, the Department of Justice/Federal Bureau of Investigation, the Director of Central Intelligence, the National Security Agency, and the Assistant to the President for National Security Affairs. The ICREA, with advice from the Department of State's Reciprocity Policy Committee, shall provide policy guidance for implementation by the Office of Foreign Missions or other appropriate organizations on proposals for foreign real estate acquisitions by lease or purchase, that present a threat to US telecommunications and automated information systems security or are of counterintelligence interest. (U)

13. The functions of the PD-24 Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the PD-24 Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively. (U)

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

9 9 COPIES

CONFIDENTIAL

CIA

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

14. Except for ongoing telecommunications protection activities mandated by and begun under PD/NSC-24, that Directive is hereby superseded and cancelled. (U)

COPY 9 OF 9 COPIES

CONFIDENTIAL

Approved For Release 2006/01/12 : CIA-RDP87B01034R000700080018-2

CONFIDENTIAL