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:

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)

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)