NSC/PD-24 DRAFT NSDD

1. Established the national policy for the protection of telecommunications ONLY.	1. Expanded to include Automated Information Systems	1. The implementation of the proposed NSDD by departments/agencies (Treasury and Energy for example) where all information handling systems (including telecommunications) are under centralized management will have minimum impact. The other civilian and military organizations will have difficulty implementing the proposed NSDD because of the diversified management of telecommunications and automated information systems. Within the Agency, OC is responsible for telecommunications and the automated systems used in support of telecommunications. ODP and OS/ISSG are responsible for the security of the remainder of the automated information systems.
2. The secretary of Defense was designated as the Executive Agent for Communications Security (COMSEC) (para 4.c). The National Communications Security Committee (NCSC); chaired by the Assistant Secretary of Defense for Communications Command, Control and Intelligence; was established as a national COMSEC framework for the conduct of COMSEC activities within the Government. NSA was a voting member of the NCSC and the charter functions of NSA were clearly defined.	2. The Secretary of Defense is designated as the Executive Agent of the Government for Telecommunications and Automated Systems Security. The Director, National Security Agency is designated as the National Manager for Telecommunications and Information Systems Security and is responsible for carrying out the responsibilities for the Secretary of Defense as Defense as Executive Agent. The NCSC is replaced by the National Telecommunications and Information Systems Security Committee with an expanded membership. A Steering Group consisting of the Secretary of Defense, the Director of Central Intelligence, the Director of OMB, and chaired by the Assistant to the President for National Security Affairs is established to oversee the implementation of the NSDD.	2. Under PD-24 the Director, NSA was a coequal with nine other regular members of the NCSC. With the chairmanship of the NCSC at the AsstSec Def level NSA could not unduly influence national standards or priorities. Under the proposed NSDD the Director of NSA will have a predominant role in determining the future of telecommunications and automated information systems utilization within the Government. The designation of the Director, NSA as the National Manager for Telecommunications and Information Systems Security should be stricken from the proposed NSDD. This is a significant reduction in the authorities of the DCI.

CONFIDENTIAL

OSD REVIEW COMPLETED

NSA review completed

NSC review completed

3. Provided for "a permanent interagency group, under the chairmanship of the Department of State, be established consisting of representatives of the Executive Office of the President, the Director of Central Intelligence, the Department of Defense, National Security Agency and the Department of Justice/Federal Bureau of Investigation to review and if necessary to deny real estate acquisitions through lease or purchase by the USSR and other Communist countries that present a potential serious threat to U.S. telecommunications security. All foreign government leased or owned facilities in this country should be evaluated as to their possible use for intercept operations."	3. The only mention of this group is contained in paragraph 13 "Responsibility for the Interagency Committee On Real Estate Acquisition is transferred to the Office of Foreign Missions pursuant to PL 97-241, 24 August 1982."	3. The thrust of PD-24 was to reduce or eliminate the vulnerability of unclassified information being passed via microwave and to ensure that classified or unclassified but sensitive information was protected by adequate cryptographic systems. This thrust is lost in the proposed NSDD.
4. PD-24 did not specifically address automated information systems.	4. Automated information systems are incorporated into the proposed NSDD without adequate definition of what is to be covered (computers, word processors, etc.). There are oblique references to a security architecture for systems without any specifics.	4. There are a number of interagency committees that are concerned with computer security under the auspicies of SECOM and the Department of Defense. If the proposed NSDD is approved, Director, NSA will be responsible for all systems. NSA has not demonstrated an expertise in this field.
5. PD-24 very obliquely addresses threat assessments.	5. The proposed NSDD is very specific on threat assessments and tasks heads of departments and agencies to provide any information requested by NSA to determine the vulnerability of telecommunications and automated information systems.	5. The exceptions under paragraphs 7 and 11 are not adequate to resist Director, NSA tasking.

NSC/PD-24	DRAFT NSDD	REMARKS
6. Paragraph 4.g states that "the heads of all departments and ageancies of the Federal Government shall organize and conduct their communications security and emanations security activities as they see fit subject to the provisions of law, the provisions of this and other directives..."	6. Paragraph 6.a states that as the National Manager for Telecommunications and Information Systems security the Director, NSA shall "empirically examine" government telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Paragraph 11.b states that "nothing in this directive shall give the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnal or facilities of other departments and agencies without the approval of the head of such department or agency, nor to request or collect information concerning their operations for purposes not provided for herein."	6. Although the wording of paragraph 11.b would imply that the Director, CIA could deny Director, NSA access to CIA facilities to "empirically examine" our telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation, it has been our experience that NSA is very aggressive in pursuing this objective. The finalization of the MOU with NSA on the interface of the CIA secure phone system with the NSA system was delayed several years because NSA insisted on the right to inspect the Agency system for compliance with NSA directives. The revision of DCID-1/16 also contains language that would permit NSA to inspect our telecommunications network to ensure compliance with NSA standards. NSA is unwilling to accept certification from the Director, CIA that the Agency is in compliance with national standards without an "empirical examination." The original draft of the NSDD contained the following language in paragraph 11.b: "Nothing in this directive shall give the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel, facilities, or internal operations of other departments and agencies without their approval." This wording was changed at the insistence of the Agency representative to the working group that prepared the proposed NSDD to ensure that any request by Director, NSA to inspect Agency facilities was addressed to the Director, CIA rather than some unnamed operating official, who might not appreciate the implications of such a request.