U.S. GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 A.M., EST
THURSDAY, JUNE 27, 1985

STATEMENT OF

WARREN G. REED

DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

ON

THE POTENTIAL IMPACT OF NATIONAL SECURITY DECISION DIRECTIVE (NSDD) 145 ON CIVIL AGENCIES

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the potential impact of National Security Decision Directive (NSDD) 145[1] on civil agencies that are not normally perceived as part of the national security establishment. We will also provide a status report on how well the directive addresses recommendations made by this Subcommittee in its April 1984 report on computer security and privacy.[2] I have with me Mr. William Franklin, Associate Director, and Dr. Harold Podell, Group Director, from the Information Management and Technology Division and Mr. Raymond Wyrsch, Senior Attorney from our Office of General Counsel.

On October 17, 1983, I testified before your Subcommittee on problems that we found in executive agencies concerning inadequate federal information security policy. In particular, I stressed the need for revising federal guidance and included a recommendation to specify when executive agencies must provide the same level of protection for sensitive information as they do for information classified for national security.

In preparing for this testimony, we had discussions with government officials who had key roles in authoring and implementing the directive being examined today. We also drew, to a limited extent, from our on-going work for your Subcommittee that addresses

[1] NSDD 145, National Policy on Telecommunications and Automated Information Systems Security, dated September 17, 1984.

[2] Computer and Communications Security and Privacy; April 1984 report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology.

the security status of major information systems. Our principal basis for examining this directive was your 1984 report.

In that report, you expressed concern that both public and private computer and telecommunications systems associated with such areas as banking, entitlement programs, law enforcement, and industrial processes need additional protection along the lines that the defense establishment has traditionally provided for its national security information. Such additional protection requires an appropriate mixture of physical, technical, and administrative security measures.

You also highlighted a lack of central leadership in establishing national policies for the protection of critical national systems of government. Specifically, you noted weaknesses in federal policy for computer and telecommunications security. OMB and other central agencies, who traditionally have had this responsibility, were chided for falling short in security management. In reinforcing your concern, you cited a variety of weaknesses associated with safeguarding these key computer and telecommunications systems. Inadequacies were noted in such areas as research and development, measures to prevent unauthorized access to critical systems, personnel training, and a data classification structure for non-national security data, etc.

Your report culminated in a variety of recommendations to Congress and the Administration, which were intended to strengthen federal leadership. The recommendation to the Congress called for the establishment of a National Commission to examine the legal, economic, institutional, social, and technical aspects of safeguarding computerized resources and other key issues. The Congress has not yet acted on this recommendation.

Recommendations to the Administration generally called for an immediate assessment and analysis of problems associated with critical national systems, as well as a strengthening of the organizational arrangements, so that national policies could be developed and implemented to ensure appropriate safeguards for critical national systems.

Executive actions related to Subcommittee report recommendations

Two independent Administration initiatives, both of which were started before the Subcommittee's April 1984 report, address several Subcommittee report recommendations.

First, the Department of Defense (DOD) developed NSDD 145, which was signed by the President and issued on September 17, 1984. The NSDD objectives include "assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information." This initiative established an organizational structure to guide the conduct of national activities directed toward safeguarding such systems.

This structure consists of four organizational components. The Systems Security Steering Group, which is responsible for overseeing the directive and ensuring its implementation, is chaired by the Assistant to the President for National Security Affairs and has six Administration department or agency heads. The second component, the National Telecommunications and Information Systems Security Committee (NTISSC), is chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence-C3I). This committee was established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement NSDD 145. The NTISSC has 22 members, of which 10 are from DOD agencies. The third component is the Executive Agent for the Government for Telecommunications and Automated Information Systems Security (in this case, the Secretary of Defense). The Executive Agent acts in accordance with policies and procedures established by the Steering Group and the NTISSC. The fourth component is the National Manager for Telecommunications Security and Automated Information Systems Security (in this case, the Director of the National Security Agency). The National Manager is responsible to the Secretary of Defense as Executive Agent for carrying out the Executive Agent's responsibilities. Attachment I lists the members of the various components.

The remaining Executive Branch initiative was an effort by the Office of Management and Budget (OMB) to consolidate and update four existing circulars pertaining to the management of federal information resources, including computer and telecommunications security. This draft circular, released for public comment on March 15, 1985, is intended to further implement various statutory and administrative provisions and policies concerning general information policy, information technology, security, privacy, and maintenance of federal records. OMB is now evaluating the comments that it has received.

Our testimony will focus on the degree to which NSDD 145 satisfies the requirements specified in the Subcommittee report and the potential impact of NSDD 145 on civil agencies.

NSDD 145 is a move in the right direction

While it is too early to provide a comprehensive assessment of how well NSDD 145 addresses, within its stated scope, the Subcommittee's recommendations, our review of this directive shows there is good potential for progress in several of the areas cited in your report. For example, a rather elaborate organizational structure has been established at high levels. The NSDD 145 organizational structure is charged with the responsibility for setting policy, providing direction, leadership, and guidance to executive agencies, increased research and development support, etc. Our review also shows that the scope of the directive falls short or is silent concerning some of the areas in your 1984 report, such as training and security awareness and computer abuse reporting.

I now would like to briefly discuss the extent to which NSDD 145 addresses the Subcommittee report's recommendations.

Federal leadership. The Subcommittee report recommended that the Administration "begin an immediate assessment of the problems and issues in order to develop a set of national policies that will ensure the protection of critical national systems relevant to government, industry, commerce, and the society." NSDD 145 partially fulfills the federal leadership recommendation by creating a single organizational entity responsible for policy, direction, and technical leadership relative to the protection of unclassified sensitive data that could affect national security. However, this directive does not cover information in national systems that is sensitive but is not considered critical to national security.

Technical and administrative guidance to federal agencies. The Subcommittee report recommended that "OMB should establish a central focus to provide technical assistance to agencies that are responsible for sensitive, non-national security data in selecting tools and techniques to protect their computer systems....General Services Administration should consider developing a manual to provide agencies with administrative guidance...." While the Subcommittee recommendation contemplated that OMB and the General Services Administration (GSA) would provide technical assistance, NSDD 145 has, in part, addressed this recommendation. Specifically it requires that telecommunications and automated system security guidance be provided to governmental departments and agencies. It does not, however, specifically cover the administrative guidance needed to complement the technical procedures.

Research and development. The Subcommittee report encouraged expanded research efforts to identify vulnerabilities that may affect future systems. NSDD 145, through the responsibilities granted the Executive Agent of the Government for Telecommunications and Automated Information Systems Security, supports the intent of the Subcommittee recommendation. In particular, the directive states, the Executive Agent should "act in accordance with policies and procedures established by the Steering Group and the

NTISSC to...conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information."

Certification of systems. The Subcommittee report identified a need for certification of hardware and software to determine their adequacy in providing the appropriate level of security. NSDD 145 gives the National Manager the responsibility to "operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems...as well as...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."

Non-national security data classification. The Subcommittee report recommended consideration of the advantages of establishing a non-national security data classification structure, such as critical sensitive, sensitive, and non-sensitive "to protect certain categories of sensitive data (e.g., financial, medical, inventory systems, etc.) in the Federal Government." Although NSDD 145 does not specifically address the data classification issue, we are aware of working groups created as a result of NSDD 145 to address key issues, such as a classification structure for sensitive data, which affects the national security interest.

The three Subcommittee report recommendations that are not specifically addressed by the directive concern (1) threats and vulnerabilities, (2) training and security awareness, and (3) computer abuse reporting. However, depending on how NSDD 145 is implemented, these recommendations could be partially addressed by actions taken under the previously discussed recommendations.

On the positive side, the NSDD 145 initiative represents progress by the Administration in partially fulfilling the intended purpose of your report through the institution of improved management mechanisms. However, it is not clear whether NSDD 145 is intended to be the Administration's mechanism for implementing recommendations of your report. This concern is reinforced by discussions we had with key Administration officials. For those who were active in authoring and implementing NSDD 145, it's clear that it was an uphill struggle to get the directive issued in the first place, and they seemed to be somewhat positive in satisfying the concerns expressed in your Subcommittee report. Other officials, particularly those who have the traditional responsibility for providing leadership in this very important area, seem to be taking a "wait-and-see" attitude. So, the bottom-line question here is whether NSDD 145 is or should be the mechanism for dealing with appropriate safeguards of national systems across all of government or only those with relevance to national security as it is currently intended. Now I would like to discuss two issues that are relevant to this question.

ISSUES REQUIRING CLARIFICATION

The first issue concerns a lack of definition for unclassified information considered sensitive with a national security interest and sensitive information that does not affect national security.

My second concern is the potential confusion as to the responsibility for computer and telecommunications security management in the federal government.

Scope of NSDD 145 Unclear

NSDD 145 has established a new category of information "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest..." without clearly defining the types of information that would be included in this category. Our concern is that if the Steering Group defines this broadly it could significantly affect the way information contained in computer and telecommunications systems maintained by civil agencies and by commercial interests must be handled. For example, unclassified sensitive civil agency information affecting national security interests could include hazardous materials information held by the Department of Transportation, flight safety information held by the Federal Aviation Administration, and monetary policy information held by the Federal Reserve.

Unclassified sensitive information not affecting national security is not addressed by NSDD 145, although it was never intended to do so and we are not necessarily advocating NSDD 145 do so. Information in this category could include such items as earnings and beneficiary information held by the Social Security Administration and financial information held by the Securities and Exchange Commission.

We believe that the Administration needs to clearly define the types of information that fall under the coverage of NSDD 145 and initiate action to address sensitive government information outside the purview of NSDD 145. In so doing, the Administration should, among other things, "clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security," as recommended by GAO in 1982.[3]

Potential for confusion as to who has the responsibility for information security in the government

NSDD 145 establishes a centralized organizational structure with designated responsibilities for policy development and implementation for telecommunications and automated information systems that process classified national security information and other sensitive information. Compromising this information could affect national security.

Depending upon how broadly or narrowly NSDD 145 is applied, the implementation of the directive may lead to confusion as to the responsibility for information security in the government. In this regard, the term "national security interest" is not defined in the directive, but the clear implication is that the directive is intended to extend to civil agencies' information systems.

On the other hand, collectively, OMB, GSA, and the Department of Commerce, on the basis of statutory and administrative directive, are responsible for establishing the necessary policies,

[3] GAO report Federal Information Systems Remain Highly Vulnerable To Fraudulent, Wasteful, Abusive, And Illegal Practices, (MASAD-82-18, dated Apr. 21, 1982).

principles, standards, and guidelines that executive agencies must implement to have an efficient and effective information security program.

Let me give you two examples where confusion over agency responsibilities may arise. First, the Brooks Act (40 U.S.C. 759) gave OMB general oversight responsibility over Commerce and GSA activities in carrying out their respective responsibilities. In 1978 OMB issued OMB Circular No. A-71, Transmittal Memorandum No. 1,[4] setting forth the responsibilities for the development and implementation of computer security programs by executive agencies. The Paperwork Reduction Act of 1980 (44 U.S.C. 3504) broadened OMB's information security program responsibilities as part of its leadership role in information resources management (IRM).

In contrast, NSDD 145 sets up a Systems Security Steering Group to act as the central organization to oversee the implementation of this directive. We are concerned that in implementing this leadership responsibility, the Steering Group could issue policy that creates questions in regard to OMB's responsibility for federal IRM leadership.

Second, the National Bureau of Standards (NBS) is responsible for developing and issuing computer security standards and guidelines. In contrast, NSDD 145 gives the Executive Agent the authority for approving and providing minimum security standards for telecommunications and automated information systems. Further,

[4] Security of Federal Automated Information Systems, Circular No. A-71, Transmittal Memorandum No. 1, dated July 27, 1978.

the directive requires NBS to submit all security-related standards and guidance affecting national security to the Steering Group for review and approval.

SUMMARY AND OBSERVATIONS

NSDD 145 is a positive step for establishing a policy framework for the protection of classified and sensitive information affecting national security and is in line with the major thrust of the Subcommittee report, as it relates to sensitive, unclassified information with a national security interest.

There is also an area of information outside the scope of NSDD 145 which must be addressed. This is sensitive information without a national security impact. Determining the appropriate mechanism for addressing this information involves tradeoffs among economic, political, and social implications, such as the impact of security measures on agencies' ability to freely exchange information in support of their missions.

If resolution of this issue favors expanding the scope of NSDD 145 to cover the full range of critical systems, then the Administration must be sensitive to political and social concerns that are likely to be expressed by government, as well as non-government, entities. The number of military organizations represented on the NTISSC and related subcommittees could cause complications, given the traditional notion that the military should not unnecessarily interfere with civilian agencv operations. Irrespective of the approach taken, implementation actions must be adjusted to ensure the spirit of the Subcommittee report recommendations is being covered or addressed.

Regardless of how the above issue is resolved, potential confusion may result due to other existing executive agency organizational responsibilities established by laws and regulations.

Our on-going work examining the status of security problems in the civil agencies, reinforces the need to protect critical national systems identified in your 1984 report. It's not clear whether the administration has pinpointed your recommendations as a target objective.

In conclusion, the Administration is aggressively pursuing the protection of information related to national security and in a sense seems to be waiting to see if the NSDD 145 initiatives will address other issues emphasized in your 1984 report. This could be a high risk approach towards achieving the objectives of your Subcommittee report.

- - - - -

This completes my prepared statement. We would be pleased to answer any questions.

ORGANIZATIONAL STRUCTURE ESTABLISHED BY NSDD 145--
NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY

The Systems Security Steering Group

--The Assistant to the President for National Security Affairs, Chairman

--The Secretary of State

--The Secretary of Treasury

--The Secretary of Defense

--The Attorney General

--The Director of the Office of Management and Budget

--The Director of Central Intelligence

The National Telecommunications and Information Systems Security Committee (NTISSC)

--Assistant Secretary of Defense (Command, Control, Communications and Intelligence--C3I), Chairman

--Voting representative of each member of the Steering Group

--The Secretary of Commerce

--The Secretary of Transportation

--The Secretary of Energy

--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, Defense Intelligence Agency

--Director, National Security Agency

--Manager, National Communications System

<u>The Executive Agent of the Government for Telecommunications and Automated Information Systems Security</u>

--The Secretary of Defense

<u>The National Manager for Telecommunications Security and Automated Information Systems Security</u>

--The Director, National Security Agency