UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 AM, EST
WEDNESDAY, OCTOBER 30, 1985

STATEMENT OF

WILLIAM S. FRANKLIN

ASSOCIATE DIRECTOR

INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

AND THE

SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

H.R. 2889

Mr. Chairman and Members of the Subcommittees:

We are pleased to be here today to provide our views on H.R. 2889 entitled the "Computer Security Research and Training Act of 1985." I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of the General Counsel.

We have long been interested in ensuring the security of automated information systems, and, during the past decade, have issued over 40 reports related to information systems security. As stated in the bill, information stored in government computers and transmitted over connecting networks is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption. Studies of computer-related fraud and abuse in government agencies show a costly and widespread problem of significant proportions.

In developing this statement, we drew upon our June 27, 1985, testimony before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on the potential impact of National Security Decision Directive (NSDD) 145[1] on civil agencies[2] and our September 18, 1985, testimony before the House Committee on Government Operations which provided our views

---

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

[2]Statement of Warren G. Reed, Director, Information Management and Technology Division, U.S. General Accounting Office, before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on the Potential Impact of National Security Decision Directive (NSDD) 145 on Civil Agencies.

on H.R. 2889.[3] Also, we drew upon our testimony given yesterday before the Subcommittee on Transportation, Aviation and Materials, on the status of computer security of selected information systems in civil agencies.[4]

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program in the federal government and the requirement that each federal agency provide mandatory periodic training in computer security. In this regard we pointed out in our testimony yesterday that only 2 of 25 systems in the agencies surveyed have a formal security training program. There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage, processing, and transmission. We further believe that the bill can be effectively used as a vehicle for addressing other related computer security management, research, and training issues, as identified in previous GAO reports and testimony, and in the April 1984

---

[3]Statement of Milton J. Socolar, Special Assistant to the Comptroller General, U.S. General Accounting Office, before the Subcommittee on Legislation and National Security, House Committee on Government Operations, on Computer Security Research and Training Act of 1985, H.R. 2889, dated Sept. 18, 1985.

[4]Statement of William S. Franklin, Associate Director, Information Management and Technology Division, U. S. General Accounting Office, before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, on Automated Information Systems Security in Federal Civil Agencies, dated Oct. 29, 1985.

report of the Subcommittee on Transportation, Aviation and Materials.[5] In particular, the Subcommittee report recommended that "...the Administration...establish a central focus...to ensure that all facets of computer security are addressed...." As we stated in our testimony on this bill before the House Committee on Government Operations, we must have a clear understanding of the levels of security required for the range of information involved, and we must have clearly established lines of responsibility and authority. Right now there is considerable confusion in both of these areas.

We pointed out to the Committee that until recently the Department of Defense (DOD) developed computer and telecommunications security standards primarily for national security information classified pursuant to Executive Order 12356. Unclassified information standards are provided by the National Bureau of Standards (NBS) pursuant to the Brooks Act and provisions of Executive Order 11717. The Office of Management and Budget (OMB) and the General Services Administration (GSA) also have major statutory responsibilities for computer and telecommunications policy and standards--OMB pursuant to the Brooks Act, the Paperwork Reduction Act of 1980, and its general mandate for oversight of executive

---

[5]Computer and Communications Security and Privacy (Report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, dated Apr. 1984.)

branch activities, while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No. 1.[6]

In September 1984, the White House issued NSDD 145, which establishes a Systems Security Steering Group as the focal point for both military and civilian information systems security. Together with an interagency committee, Executive Agent, and the National Manager, the Steering Group is to establish and coordinate policies and review and approve budgets for computer and telecommunications security efforts throughout the government. This structure created by NSDD 145 partially fulfills the federal leadership recommendation in the Subcommittee's April 1984 report. However, the directive does not cover information in national systems that is sensitive but is not considered critical to national security.

The directive provides for safeguarding from hostile exploitation systems that process and communicate sensitive information. And here the definition of sensitive information has been broadened to include any information affecting national security interests whether classified or unclassified. It puts DOD and the civilian lead agencies in the same arena for large segments of information. However, this occurs without a clearly established division of responsibilities, at least until the scope of the new definition of sensitive information is specified.

---

[6]"Security of Federal Automated Information Systems," issued July 27, 1978.

NSDD 145 does recognize that OMB, NBS, and GSA have major functions to carry out with regard to the security of information in automated systems, but the directive places ultimate control over the functions exercised by those agencies in the administrative structure it established. Activities of the civilian agencies are all made subject to NSDD 145 approval mechanisms. Therefore, there is a potential for confusion regarding similar mechanisms established by legislation for NBS, OMB, and GSA. The NSDD 145 mechanisms diffuse the recommendation for a central focus contained in the April 1984 Subcommittee report.

The following provisions of H.R. 2889 overlap similar provisions of National Security Decision Directive 145. Section 3 of H.R. 2889 provides for NBS to

--perform research and conduct studies to determine the nature and extent of computer security vulnerability in federal agencies and their contractors;

--devise administrative, management, and technical procedures and practices designed to protect the information stored, processed, and transmitted by government computers; and

--develop guidelines for use by federal agencies in training their employees, and the employees of their contractors and of other organizations whose computers interface with government computers, in computer security awareness and good security practice.

NSDD 145 gives the Director, National Security Agency, as National Manager, responsibilities to

--conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information;

--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. No monitoring shall be performed without advising the heads of the agencies departments or services concerned; and

--review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

These provisions would seem to provide for different agencies to perform similar functions. However, it is difficult to judge the precise extent of overlap that enactment of H.R. 2889 would engender, since the full range of NSDD 145 and its overall applicability to civilian agencies is unclear.

While we support the need for a comprehensive computer security research and training program as proposed by H.R. 2889, we would suggest, that since computer security research and training programs are carried out by DOD for all federal agencies for both classified and much unclassified information, that a clear understanding of DOD's role versus the roles of OMB, GSA, and NBS be established in conjunction with consideration of H.R. 2889.

In conclusion, we support the intent of H.R. 2889. We believe deliberations over this bill provide a good opportunity for the Congress to consider establishing a central focus for computer security in the federal government, and at the same time preserve more of the traditional roles of the various executive agencies as provided for in existing legislation.

More importantly, the broad leadership role that NSDD 145 assigns predominantly to DOD raises basic questions concerning the extent to which the defense establishment should be involved in policy formulation and program administration within the government's civilian agencies. There can be no question that there is unclassified information stored in government computers and transmitted through telecommunications systems, the unauthorized disclosure or disruption of which could affect our national interests. It does not follow that DOD must be responsible for deciding what should be done to protect this information. The assignment of that responsibility is an issue of long-range importance that should be thoroughly considered by the Congress.

- - - - -

That completes my prepared statement, Mr. Chairman. We would be pleased to answer any questions.

32602