~~32279~~ 127934

UNITED STATES GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 10:00 AM, EST
SEPTEMBER 18, 1985

STATEMENT OF

MILTON J. SOCOLAR

SPECIAL ASSISTANT TO THE COMPTROLLER GENERAL

BEFORE THE

SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY

COMMITTEE ON GOVERNMENT OPERATIONS

HOUSE OF REPRESENTATIVES

ON

COMPUTER SECURITY RESEARCH AND TRAINING ACT OF 1985

H.R. 2889

Mr. Chairman and Members of the Subcommittee:

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." 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 system 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.

We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research and training program to address problems of computer security in the federal government. 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 and transmission. But in order to move ahead efficiently we must have a clear understanding of the levels of security required for the range of information involved, and we must have established lines of responsibility and authority that are clear. Right now there is considerable confusion on both of these counts.

Until recently the Department of Defense developed computer and communication 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 communication policy and standards--OMB pursuant to the Brooks Act, the Paperwork Reduction Act of 1980, and its general mandate for oversight of executive branch activities, while GSA's responsibilities stem from the Brooks Act and OMB Circular A-71, Transmittal Memorandum No.1.

In September 1984, the White House issued National Security Decision Directive 145, which establishes a Systems Security Steering Group as the focal point for both military and civilian information security. Together with an inter-agency committee, Executive Agent, and the National Manager the Steering Group is to establish and coordinate policies and review and approve budgets for computer and communications security efforts throughout the government. The directive provides for safeguarding from hostile exploitation systems that process or 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. NSDD 145 puts DOD and the civilian lead agencies in the same arena for large segments of information, but without a clearly established division of responsibilities at least until the scope of the new definition of sensitive information is specified. 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.

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 these 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 this connection, it should be noted that there is a potential that we will commit ourselves to the development and

teaching of inordinately expensive approaches to computer security. DOD, in its approach to security, seeks to counter identified or perceived threats to the national defense, treating costs as a decidedly secondary factor in determining the degree of protection required. The National Bureau of Standards, on the other hand, emphasizes a risk management approach that uses costs as a primary determinant. Now that NSDD 145 has created a category of information designated as sensitive unclassified information there is a potential, if not a likelihood, with DOD taking the lead, for excessive expenditures to protect unclassified information.

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 communication 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.

3219