United States General Accounting Office 133500

GAO

Testimony

For Release
on Delivery
Expected at
10:00 a.m. EST
Wednesday
February 25,
1987

THE COMPUTER SECURITY ACT OF 1987

H.R. 145

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

039505

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to provide our views on H.R. 145, entitled the "Computer Security Act of 1987."

We support the bill's purpose of providing for the security and privacy of sensitive information in federal computer systems through the development of security standards, research, and training, and the establishment of security plans by all operators of federal computers systems that contain sensitive information. There can be little doubt that such initiatives are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage and transmission.

Much of the underlying purpose of H.R. 145 is now addressed in National Security Decision Directive (NSDD) 145, which assigns the Department of Defense primary responsibility. While the approach adopted by H.R. 145 allows full use of the technical expertise of the National Security Agency (NSA), among others, in developing methods of protection, it gives a civil agency, the National Bureau of Standards (NBS), final responsibility for developing and mandating these methods, except for classified national security information and certain other defense-related information. NBS already has a broad range of similar standards responsibility pursuant to the Brooks Act.

I recognize that NBS' capability will have to be significantly enhanced if it is to discharge adequately the responsibilities placed upon it by H.R. 145. I recognize too that DOD, by virtue of its available staff and experience with classified national security information and cryptographic practices, has capability that would be of value in accomplishing the overall desired objectives. Nevertheless, under NSDD-145, DOD would direct government policies relating to protection and control of a vast body of information, which, although unclassified, might be deemed sensitive. And that is a matter of some concern.

For some time, the government has sought to deny Eastern Bloc countries unclassified products of U.S. technology , such as advanced computers and conventional weapons, that have possible military or national security significance. More recently, this effort has been extended beyond the tangible products of technology to include information useful in the duplication of that technology. In the DOD Authorization Act of 1984, for example, the Secretary of Defense was given authority to withhold from public disclosure unclassified technical information with military or space application.

NSDD-145, and its implementing policy on sensitive information, extend these efforts to include a broad range of information which resides in computer databases and is transmitted electronically, but which is not related to national security. The motivation for

this extension is the perception that foreign intelligence, Allied as well as Eastern Bloc, has the capability to access U.S. government and private sector databases and to intercept telecommunications that are unclassified in order

-- to collect information that, separated, is benign but that aggregated is inimical to U.S. interests,

-- to acquire proprietary information on U.S. technology that may be of economic benefit to their nationals, and

-- to obtain information on planned activities of the U.S. government and individual corporations that can be used to the detriment of U.S. interests.

In response to this threat, NSDD-145 and its implementing policy on sensitive information are intended

-- to focus and coordinate government-wide efforts to improve the security of telecommunications and automated information systems handling government and government-derived information which, although unclassified, is perceived as directly vital to a range of U.S. interests, including economic, financial and technological leadership, as well as national security and

-- to provide a base of technical tools, procedures, and assistance to enable the private sector to protect information that may be indirectly important to long-term U.S. interests.

NSDD-145 was issued on September 17, 1984. It established a steering group, chaired by the Assistant to the President for National Security Affairs, and a committee, chaired by the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (C3I), to furnish leadership for improved telecommunications and automated information systems security. The Director of NSA is designated "national manager" with authority to review and approve all standards, techniques, systems, and equipment for telecommunications and automated information systems.

In testimony before this Committee on September 18, 1985, we expressed concern over the open-ended scope of NSDD-145 and its potential for permitting the involvement of DOD in the protection of government information that did not involve national security -- areas where, under existing legislation, NBS and the civil agencies have had the primary role. The Assistant Secretary of Defense for C3I asserted in those same hearings that NSDD-145 was directed solely at the protection of information affecting national security interests of the United States.

On October 29, 1986, the scope of "sensitive" information covered by NSDD-145 was defined in policy issuance number 2 as including sensitive but unclassified information pertaining to national security or other federal government interests. "Other federal government interests" were explicitly defined to be "those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens."

Alarmed by perceived potential government curtailment of free access to unclassified information by U.S. nationals, various groups have expressed concerns. For example, according to articles in the press:

-- The Legislative Counsel for the American Civil Liberties Union has said that by restricting access to databases, "the U.S. is moving more and more toward the militarization of the flow of scientific information" and thereby jeopardizing freedom.

-- The former General Counsel to the U.S. Privacy Protection Study Commission has indicated that "any change in the present status of unrestricted and open access to general

information databases raises major First Amendment issues."

-- The Information Industry Association has urged Secretary Weinberger to withdraw the new sensitive but unclassified information category on the grounds that Pentagon controls would hurt the business of information vendors.

It is important to keep in mind when establishing computer security that many legitimate users of government and private automated data files now enjoy open access to full databases. Will these users be able to pursue their interests if access is curtailed because of a determination that the files they search are sensitive? Designation of a computerized file as sensitive would, under either NSDD 145 or H.R. 145, call only for protection of data from unauthorized disclosure and not for any determination as to who might have legitimate access thereto. Yet, it is inevitable that the very designation of files as sensitive, which places them under security measures, would result in limitations on access -- restricting the kind of free flow of information that is of vital interest to our society. How to achieve balance between the need for security and the benefits which flow from a free exchange of information is an issue of utmost importance.

Any decision to define some set of unclassified government information as "sensitive," and to determine what restrictions on

access are appropriate for its protection, involves trade-offs among many factors, including a clear interest in maintaining the free flow of government information, the impact on U.S. technology development, and economic value to the private sector. In light of the extent to which DOD is the guiding force behind NSDD-145, we remain concerned as to whether the range of trade-offs will be appropriately considered in making these decisions -- especially in those areas not involving national security. NSDD-145 and implementing policy issuance number 2, with its open-ended definition of "sensitive" information and with a decision structure dominated by DOD and NSA, provide a degree of influence and control to the military over a great deal of information that lies in the domain of civilian interests, a degree of control that is worrisome.

H.R. 145 appropriately places responsibility for the protection of unclassified but sensitive, non-national security information with the civilian side of government, vesting authority in the Secretary of Commerce and NBS. Even so, H.R.145 does not go far enough in ensuring that abuses will not occur through the overzealous categorization of systems as "sensitive." The bill needs to be strengthened to ensure that appropriate safeguards surround any tendency toward an unwarranted restriction of access to unclassified data. The bill should explicitly spell out that its provisions are not to be construed as in any way modifying the

availability of information under the terms of the Freedom of Information Act. Also, it might be well to require advance public notification of an intent to designate a particular data or telecommunication system as sensitive ... the rationale behind that determination ... any restrictions contemplated on public access to that system ... and to provide an opportunity for public comment. This kind of visibility would facilitate public participation and Congressional oversight and should significantly contribute to the prevention of abuses.

I would close by saying that in recognizing the need to provide security for computerized data systems, we have to look beyond terms that express the limited purpose of safeguarding unclassified information from inadvertent disclosure. There simply is too much opportunity and tendency toward excessive interference with the free exchange of information for us to rely idly upon the good intentions of those who would assume responsibility for defining government policy on this most sensitive issue.