United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
10:00 a.m. EDT
Thursday
May 4, 1989

National Institute of Standards and Technology and the National Security Agency's Memorandum of Understanding on Implementing the Computer Security Act of 1987

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

Mr. Chairman and Members of the Committee:

We are pleased to be here today to discuss the recently signed Memorandum of Understanding (MOU) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in implementation of the Computer Security Act of 1987 (P.L. 100-235). Although the MOU does not legally bind the Secretary of Commerce, it nevertheless will likely define the future relationship between NIST and NSA on matters pertaining to the act.

At issue is the degree to which responsibilities vested in NIST under the act are being subverted by the role assigned to NSA under the memorandum. The Congress, as a fundamental purpose in passing the act, sought to clearly place responsibility for the computer security of sensitive, unclassified information in a civil agency rather than in the Department of Defense. As we read the MOU, it would appear that NIST has granted NSA more than the consultative role envisioned in the act.

Although officials from both agencies may adequately explain those provisions we consider vague or inappropriate as presently worded, the MOU at a minimum requires clarification to provide greater assurance that NIST will be working with NSA as contemplated by the act; that is, that NSA will serve more as consultant to the directive authority of NIST in the sphere of sensitive, unclassified information.

Computer Security Act of 1987

The general purpose of the Computer Security Act of 1987 was to improve the security and privacy of sensitive, unclassified information in federal computer systems by providing a means of establishing minimum acceptable security practices. To do so, the act made the National Bureau of Standards (now NIST), responsible for developing standards and guidelines needed to cost-effectively protect federal sensitive information, drawing on NSA's technical advice and assistance where appropriate. Under the act, operators of these systems must establish security plans and periodically train everyone who manages, uses, or operates them. In developing these provisions, the Congress considered, among other things, the need for greater civil agency control over these systems.

The act directs the Secretary of Commerce to promulgate standards and guidelines for federal computer systems, making such standards compulsory and binding to the extent the Secretary determines necessary to improve system efficiency, security, and privacy. The President may disapprove or modify such standards and guidelines if he deems it in the public interest. Further, the act specifies that the President may not delegate this responsibility. If the President disapproves or modifies the standards he must promptly notify the House Government Operations and the Senate Governmental Affairs Committees and publish a notice in the Federal Register.

Summary of the Memorandum

The MOU describes the roles and responsibilities of NIST and NSA in implementing the Computer Security Act of 1987. NIST responsibilities include appointing a Computer Security and Privacy Advisory Board; drawing on NSA's computer system technical security guidelines to the extent NIST determines they are consistent with requirements for protecting sensitive information; recognizing NSA certified ratings of evaluated trusted systems without requiring additional evaluation; and developing telecommunication standards for protecting sensitive unclassified data, drawing on NSA expertise and products to the greatest extent possible.

NSA's responsibilities include providing to NIST technical guidelines in trusted technology, telecommunications security, and personal identification; conducting research and development in trusted technology, telecommunications security, cryptography, and personal identification methods; responding to NIST requests on all matters related to cryptography; establishing standards and endorsing products for application to secure military systems; and, upon request by federal agencies, their contractors and other government sponsored entities, assessing the hostile intelligence threat against federal information systems and providing technical assistance and recommending endorsed products to secure systems against that threat.

The MOU also specifies that NIST and NSA agree to (1) jointly review agency plans for security and privacy submitted pursuant to the Act; (2) exchange technical standards and guidelines, as necessary; (3) work together to avoid duplicate effort and maintain an open dialogue; (4) exchange work plans annually on all research and development projects involving protection of systems that process sensitive or other unclassified information; and (5) establish a Technical Working Group to review and analyze issues of mutual interest.

Concerns About the Memorandum

The act recognizes a significant role for NSA in computer security and privacy. Portions of the memorandum, however, are not clear about the respective roles of NSA and NIST. In particular, the scope of activities for the Technical Working Group it establishes is unclear, raising uncertainties about the extent of NSA involvement in NIST functions. Other provisions raise questions as to whether the NIST and NSA roles are appropriately set forth including (1) the inclusion of research and development activities for NSA but not for NIST, (2) the automatic acceptance of NSA evaluations of Trusted Systems, and (3) the NSA evaluation of security programs. I will discuss each these concerns individually.

Section III.5 of the MOU establishes a Technical Working Group to

review and analyze issues of mutual interest pertinent to protection of systems that process sensitive, unclassified information. The group will consist of six federal employees, three each selected by NIST and NSA. Under section III.7, the group will review, prior to public disclosure, all matters regarding technical systems security techniques to be developed for use in protecting sensitive information to ensure they are consistent with the national security. If NIST and NSA are unable to resolve an issue within 60 days, either agency may raise the issue to the Secretary of Defense and the Secretary of Commerce. Such an issue may be referred to the President through the National Security Council (NSC) for resolution. The MOU specifies that no action is to be taken on such an issue until it is resolved.

These provisions appear to give NSA more than the consultative role contemplated under the act. They seem to give NSA an appeal process--through the National Security Council--leading directly to the President should it disagree with a proposed NIST standard or guideline. The act provides that the President may disapprove any such guidelines or standards promulgated by the Secretary of Commerce, that this disapproval authority cannot be delegated, and that notice of any such disapproval or modification must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs. Under section III.7 of the MOU, it appears that an avenue has been opened which would invite presidential disapproval or modification of standards and

guidelines in advance of promulgation by the Secretary without proper notification to the Congress.

We understand, however, that NIST considers that the review and appeal process provided for in III.7 excludes the working group from any approval authority over standards and guidelines. NIST apparently views the phrase "review matters ... to be developed" as limiting consideration to proposed research and development projects in new areas. NIST feels that NSA presented compelling national security concerns which warranted early review and discussion of NIST's planned computer security related research and development. If concerns arise, NSA wanted a mechanism to resolve problems before projects were initiated.

If this provision pertains only to research and development, it still gives NSA a significant role in what were to be NIST functions under the act. NSA could cause significant delay of a project NIST deems warranted, and it would appear that in matters of disagreement, Commerce has placed itself in the position of having to appeal to the President regardless of its own position.

The MOU's treatment of the research and development activities of the respective parties also gives the appearance that NSA will have dominant responsibility in the area. For example, section II.2 provides that NSA will conduct or initiate research and development programs in trusted technology, telecommunications security,

cryptographic techniques, and personal identification methods. And section I.6 states that NIST will request NSA's assistance on all matters relating to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement. We have no quarrel with these provisions. But the lack of provisions outlining corresponding NIST undertakings raises question as to whether the extent of NIST research and development activities and overall direction will be as comprehensive as the act intended.

In another example, section I.3 provides that NIST will recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation. This apparently limits NIST activities in this area and could be interpreted to require that NIST forego its own evaluation of sensitive systems in deference to NSA standards. Requiring NIST to accept the NSA standards without intervention would further erode NIST authority under the act.

A final example is section II.5 requiring NSA upon request by federal agencies, their contractors and other government-sponsored entities to conduct assessments of the hostile intelligence threat to federal information systems and provide technical assistance and recommend solutions. We are uncertain as to how this requirement relates to NIST's authority and responsibility under the act to determine the nature and extent of the vulnerabilities of sensitive

information in federal computer systems and to devise techniques for the security and privacy of sensitive information. Again, the MOU role spelled out for NSA, in the absence of a specification of NIST functions, suggests a diminution of NIST responsibilities.

In conclusion Mr. Chairman, I would say that the MOU appears to increase the burden of leadership which the Secretary of Commerce must exercise in implementing the Computer Security Act of 1987. The MOU itself is, perhaps, not as important as the sense it provides regarding the manner in which the act is being implemented. It may well be, notwithstanding the wording of the MOU, that NIST and the Secretary of Commerce will exercise strong control over their authorities and responsibilities as set forth in the act. Nevertheless, as one reviews the document itself against the language and background of the act, one cannot help but be struck by the extent of influence NSA appears to retain over the processes involved in certain areas--an influence the act was designed to diminish. While agency officials may provide explanations that would alleviate concerns raised by the language of the MOU, it would be useful at a minimum to incorporate such understandings in the memorandum itself in the interest of promoting a clearer understanding of how NIST and NSA will be working together.

- - - - -

That concludes my prepared statement and I would be pleased to answer your questions.