United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
1:30 p.m. EDT
Tuesday
July 10, 1990

Impact of the Governmentwide Computer Security Planning and Review Process

Statement of
Jack L. Brock, Jr., Director, Government
Information and Financial Management Issues
Information Management and Technology Division

Before the
Subcommittee on Transportation, Aviation
and Materials
Committee on Science, Space, and Technology
House of Representatives

GAO/T-IMTEC-90-11

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here to discuss the governmentwide computer security planning and review process implemented under the Computer Security Act of 1987. The act, which is intended to improve the security and privacy of sensitive information in federal computer systems, required agencies to (1) identify systems containing sensitive information, (2) develop and submit to the National Institute of Standards and Technology (NIST) and National Security Agency (NSA) for advice and comment a plan for each system identified, and (3) establish computer security training programs.[1] To be in compliance, approximately 60 civilian agencies submitted almost 1,600 computer security plans to a NIST/NSA review team in early 1989.

My testimony today is based on our review at 10 civilian agencies, where we assessed the planning process, the NIST and NSA review of the plans, and the extent to which the agencies implemented planned controls described in 22 plans. The issues I am discussing are described in greater detail in our report, Computer Security: Governmentwide Planning Process Had Limited Impact (GAO/IMTEC-90-48, May 1990).

[1] The act defines sensitive information as any unclassified information that in the event of loss, misuse, or unauthorized access or modification, could adversely affect the national interest, conduct of a federal program, or the privacy individuals are entitled to under the Privacy Act of 1974 (5 U.S.C. 552a).

Overall, we believe that the planning and review process had little impact on agency computer security programs. Agency officials typically described the plans developed under the process as merely "reporting requirements" rather than as tools for managing their security programs. The NIST and NSA review comments on agency plans were general and of limited use to agencies in dealing with specific computer security problems. Finally, many agencies we reviewed made little progress in implementing planned controls---a year after the initial plans were completed, only 38 percent of the planned controls had been implemented.

PROCESS HAD LIMITED IMPACT ON AGENCY SECURITY PROGRAMS

We found that a key problem with the planning and review process was that it was designed to fulfill dual and somewhat conflicting purposes---to help agencies plan as well as to meet the needs of a governmentwide reporting process involving the review of thousands of plans. The plans were designed to be brief, both to limit the risks of unauthorized disclosure of system vulnerabilities and to facilitate the NIST/NSA review. Consequently, the plans lacked important information, such as budget estimates for planned actions, needed for planning and monitoring security programs.

A number of other reasons contributed to the process's limited impact:

-- First, officials from about a third of the agencies we reviewed said that they already had more comprehensive planning processes to help them identify and evaluate security needs. As a result, the governmentwide process was largely superfluous for these agencies.

-- Second, agency officials had little time to consider their security needs in preparing the plans. This further limited the plans' usefulness and, I believe, reinforced the view that they were little more than reporting requirements. In most departments, instructions for responding to Office of Management and Budget (OMB) Bulletin 88-16, which provided guidance on preparing the plans, were issued from 4 to 13 weeks before the plans were due back to the departments. Much had to be accomplished in this time: instructions had to be sent to component agencies and from there to the managers responsible for preparing the plans; meetings had to be held to discuss the plans; managers had to prepare the plans; and the plans had to be reviewed by agency management before being returned to the department for submission to NIST and NSA. As a result, some managers had only a few days to prepare the plans.

-- Third, many agency officials misinterpreted or were confused about the guidance in the OMB bulletin. Areas of confusion included how systems were to be combined in plans, the definitions of some key terms, the amount of narrative detail, and the need to address telecommunications issues, such as network security. For example, although the guidance specified that only similar systems could be combined, some plans combined many different types of systems--such as microcomputers and mainframes--having diverse security needs and functions. Agency officials stated that they combined systems based on their understanding of the OMB guidance and NIST/NSA oral instructions.

-- Finally, since the plans contained minimal detailed information, the review feedback was general and of limited use to agency officials. The NIST/NSA review team comments focused on stating whether the plans conformed to the OMB planning guidance and on citing governmentwide guidance relating to planned security controls. However, because the plans were designed to be brief and lacked detailed information, a more comprehensive review may have been infeasible.

AGENCIES HAVE NOT IMPLEMENTED MOST PLANNED CONTROLS

The 22 plans we reviewed, initially prepared in early 1989, reported that 145 out of almost 400 security controls were not fully in place. As of January 1990, a year later, agency officials said that only 38 percent of the 145 planned controls had been implemented.[2] Controls with low implementation rates included risk assessments, security specifications, and certification. According to agency officials, budget constraints and inadequate top management support were key reasons why the planned controls had not been implemented. Some officials stated that although the planning process has made management more aware of computer security, this awareness generally has not yet resulted in increased resources for computer security programs.

REVISED DRAFT OMB GUIDANCE REFOCUSES EFFORTS

Based on the results of the planning and review process, OMB--in conjunction with NIST and NSA--issued revised draft security planning guidance in January 1990.[3] Under the draft guidance, NIST, NSA, and OMB would focus efforts on assisting and advising federal agencies on their computer security programs. Many agency officials said that they could benefit from technical assistance, especially in areas such as network security. Under the guidance, NIST, NSA, and OMB would visit agencies to discuss their security programs, plans, and other related issues and provide technical assistance as needed.

[2] About 4 percent of the 145 planned controls had target implementation dates beyond January 1990.

[3] OMB officials said that they expect to issue final revised security planning guidance in July 1990.

We believe that OMB's draft guidance creates the potential for improving computer security by going beyond planning and attempting to address agency-specific computer security problems. However, NIST, OMB, and NSA assistance efforts must be matched by agency management commitment and actions to make needed improvements. Ultimately, it is the agencies' responsibility to ensure that the information they use and maintain is adequately safeguarded and that appropriate security measures are in place and tested. Agency management of computer security is an issue we plan to address in our ongoing review of this important area.

- - - -

That concludes my statement. My colleagues and I would be glad to respond to your questions.