GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-283396

August 9, 1999

The Honorable Constance A. Morella
Chairwoman
Subcommittee on Technology
Committee on Science
House of Representatives

Subject: Information Security: Answers to Posthearing Questions

Dear Ms. Chairwoman:

This letter responds to your July 15, 1999, request that we answer questions relating to our June 24, 1999, testimony[1] on the need for stronger information security management. Your questions, along with our responses, follow.

1. Over the years, GAO has issued a number of reports on agencies' computer security practices. In your opinion, how effective has the implementation of the 1987 Computer Security Act been?

The Computer Security Act's primary objectives were to provide for (1) a computer standards program within the National Institute of Standards and Technology (NIST), (2) governmentwide computer security, and (3) training in security matters for persons involved in the management, operation, and use of federal computer systems. While a standards program and some training have been provided, governmentwide computer security has not been achieved, primarily because individual agencies have not taken the steps needed to effectively implement NIST's standards and related guidance.

In 1998, we analyzed the results of the previous 2-1/2 years' computer security audit reports (both our reports and agency inspector general [IG] reports) and found that significant weaknesses were reported for all 24 of the agencies covered by our analysis.[2] These weaknesses placed a broad range of critical operations and assets at

[1] Information Security: Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management (GAO/T-AIMD-99-223, June 24, 1999).

[2] Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAP/AIMD-98-92, September 23, 1998).

162647

great risk of fraud, misuse, and disruption. We also reported that, although a number of agencies, councils, and task forces were attempting to improve federal information security by addressing selected issues, there was no governmentwide strategy in this regard.

2. In 1998 Presidential Decision Directive No. 63 (PDD-63) was issued. Among its goals was improved information security at federal agencies. What gaps will PDD-63 fill within existing federal programs that will improve the security of federal computer systems?

During the 14 months since its issuance, PDD-63 has focused increased attention on computer security and raised awareness of our government's dependence on computer and telecommunications systems, the threats to these systems, and the significant damage to our national welfare that could ensue should these systems be successfully attacked. Most notably, PDD-63 has prompted efforts to develop a national plan, which is expected to address (1) evaluating and improving agency computer security plans and (2) developing improved capabilities for detecting and responding to serious computer-based attacks. In addition, PDD-63 recognized the interdependencies among public and private sector entities, especially as they relate to protecting our nation's computer-supported critical infrastructures. In this regard, the Directive initiated efforts to improve public-private sector cooperation. As of early August, it is too soon to determine how successful the PDD-63 efforts will be. In particular, the anticipated national plan has not yet been issued, so we cannot comment on any specific planned actions.

3. In 1998, GAO issued an Information Security Management guide that was subsequently distributed to all agencies. How does the GAO document differ from existing NIST issued guidelines and bulletins? Also, how have agencies responded to your guidelines and have they implemented your suggestions?

Our guide[3] is based on the results of our study of eight nonfederal organizations regarded as having superior computer security programs. As a result of this study, we identified a risk management cycle of activity, including 16 specific practices that these organizations told us were important to the success of their programs. These practices are consistent with NIST guidance as well as with Office of Management and Budget (OMB) guidance. In this regard, our guide complements NIST and OMB guidance and should be viewed as a supplement to their publications. The primary characteristics that distinguish our guidance from NIST's are listed below:

[3] Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

- The GAO guide focuses almost exclusively on the design and management of an effective security program. NIST's guidance also focuses on these topics, but much of it also elaborates on specific control techniques.
- The GAO guide is aimed primarily at senior federal program officials, and it emphasizes the role of these officials in ensuring that the data and systems supporting their programs are adequately protected. While some of NIST's guidance is also targeted at this audience, most of it is designed to assist agency security specialists in carrying out their often more technical responsibilities.
- The GAO guide provides illustrative examples of practices in operation at each of the eight organizations studied. NIST guidance usually does not provide such examples.

In response to the second part of your question, agencies, as well as several private sector organizations, have responded very favorably to our guide. The Chief Information Officers Council endorsed the guide for use by the federal community, and NIST issued a summary of the guide as one of its Information Technology bulletins. Several agencies, including the departments of State, Justice, and Education and the Federal Deposit Insurance Corporation have used the guide to strengthen and reorient their security programs to address the risks associated with today's highly interconnected computing environment. GAO and some IGs have incorporated the guide's principles and practices into their own information security audit criteria, so future audit results should help gauge the guide's impact. However, it is important to note that while establishing a risk management framework is a fundamental step, an effective security program also depends on other factors, such as the availability of (1) sufficient technical experts to implement and maintain an agency's security program and (2) effective software tools to combat threats like hacker intrusions.

4. You recommend independent audits of agencies' information security programs. Several years ago, OMB tasked NIST and the National Security Agency (NSA), on a one-time basis, to audit agencies. Was this audit effective and useful? Do you believe that NIST/NSA should perform these audits on a regular basis?

The effort you refer to was completed in 1992. At that time, representatives from OMB, NIST, and NSA visited 28 agencies in an attempt to gain an overview of the agencies' information security programs, raise awareness of risks, and promote compliance with existing guidance. According to a January 1992 letter to the Director of OMB from the Computer System Security and Privacy Advisory Board, the visits were enthusiastically received by the agencies and resulted in greater awareness on the part of senior officials, which, in turn, resulted in increased management support for agency computer security programs. In addition, the visits resulted in proposals for improving federal information security, most of which were incorporated in OMB's February 1996 revision of Circular A-130, Appendix III.

While reportedly serving their intended purpose, the 1992 visits were not audits because they did not involve direct observation or testing of agency security controls in operation. We have found that only through such observation and testing is it possible to reliably assess the effectiveness of agency controls and identify specific recommendations for improvement. Also, to serve as a useful measure of performance, such audits need to be performed periodically so current performance can be compared to past performance and related recommendations.

NIST and NSA should have a significant role in any such audits. Depending on the scope and frequency of audit requirements that might be imposed, this role could vary. For example, NIST and NSA could (1) perform audits at selected agencies, (2) assist agency inspectors general, especially in performing the more technical aspects of the audits, or (3) review and evaluate the quality of audits performed by others.

Should you or your staff have any questions concerning this letter, please contact me at 202-512-6412. I can also be reached by e-mail at rhodesk.aimd@gao.gov. Key contributors to this assignment were Jean Boltz and William Wadsworth.

Sincerely yours,

Keith A. Rhodes
Director, Office of Computer and
Information Technology Assessment

(511061)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001