United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Wednesday,
March 29, 2000

FEDERAL INFORMATION SECURITY

Actions Needed to Address Widespread Weaknesses

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

G A O
Accountability * Integrity * Reliability

GAO/T-AIMD-00-135

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss federal information security. Our recent audit findings in this area present a disturbing picture of the state of computer security practices at individual agencies. Our work—and the work of other audit entities—has demonstrated that many agencies' critical operations and processes are at serious risk of disruption because of weak security practices. We have designated computer security as a high-risk area, and the President's plan for protecting critical infrastructure[1] reinforces this designation.

At your request, I will discuss actions agencies can take immediately to strengthen their security programs as well as other actions required to make more fundamental and long-term improvements. Additionally, I will discuss governmentwide actions needed to support and encourage agency progress and congressional oversight of this progress.

Serious and Widespread Weaknesses Place Critical and Sensitive Operations and Assets at Risk

Computers and electronic data are indispensable to critical federal operations, including national defense, tax collection, import control, benefits payments, and law enforcement. Computers make it possible to process information quickly and communicate almost instantaneously among federal offices, outside organizations, and individuals. In addition, they make vast amounts of data accessible to anyone with a personal computer, a modem, and telephone.

However, this reliance on automated systems increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. The same factors that benefit operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on operations, possibly for purposes of fraud or sabotage or other malicious purposes. Threats of such actions are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through magazines and on computer bulletin boards. In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection,* Version 1.0, The White House, January 2000.

Recent audits show that federal systems are highly vulnerable to these risks. Our October 1999 analysis of our own and inspector general audits found that 22 of the largest federal agencies were not adequately protecting critical federal operations and assets from computer-based attacks.[2] Our most recent individual agency review, of the Environmental Protection Agency (EPA), corroborated our governmentwide analysis.[3] Our tests identified numerous security weaknesses associated with the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations. In addition, EPA's own records identified several serious computer incidents in the last 2 years. EPA is currently taking significant steps to address these weaknesses, but resolving them on a lasting basis will require substantial ongoing management attention and changes in the way EPA views information security.

EPA is not unique. Within the past 12 months we have identified significant management weaknesses and control deficiencies at a number of agencies.

- In August 1999, we reported[4] that pervasive weaknesses in Department of Defense information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data.

- In May 1999, we reported[5] that as part of our tests of the National Aeronautics and Space Administration's (NASA) computer-based controls, we successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for each orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. Having obtained access, we could have disrupted ongoing command and control operations and modified or destroyed system software and data.

[2]*Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

[3]*Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/T-AIMD-00-97, February 17, 2000).

[4]*DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999).

[5]*Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999).

- In August 1999, an independent accounting firm reported[6] that the Department of State's mainframe computers for domestic operations were vulnerable to unauthorized access. Consequently, other systems, which process data using these computers, could also be vulnerable. A year earlier, in May 1998, we reported[7] that our tests at State demonstrated that its computer systems and the information they maintained were very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses.

- In October 1999, we reported[8] that serious weaknesses placed sensitive information belonging to the Department of Veterans Affairs (VA) at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. Such findings were particularly troublesome since VA collects and maintains sensitive medical record and benefit payment information for veterans and family members and is responsible for tens of billions of dollars of benefit payments annually.

Control Weaknesses Are Similar Among Agencies

Although the nature of operations and related risks at these and other agencies vary, there are striking similarities in the specific types of weaknesses reported. The following six areas of management and general control weaknesses are repeatedly highlighted in our reviews.

- ***Entitywide Security Program Planning and Management.*** Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Despite the importance of this aspect of an information security program, we continue to find that poor security planning and management is the rule rather than the exception. Most

[6] *Audit of the Department of State's 1997 and 1998 Principal Financial Statements*, Leonard G. Birnbaum and Company, LLP, August 9, 1999.

[7] *Computer Security: Pervasive Serious Weaknesses Jeopardize State Department Operations* (GAO/AIMD-98-145, May 18, 1998).

[8] *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-05, October 4, 1999).

agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

- ***Access Controls.*** Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. They include physical protections such as gates and guards. They also include logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can execute. In many of our reviews we have found that managers do not identify or document access needs for individual users or groups, and, as a result, they provide overly broad access privileges to very large groups of users. Additionally, we often find that users share accounts and passwords or post passwords in plain view, making it impossible to trace specific transactions or modifications to an individual. Unfortunately, as a result of these and other access control weaknesses, auditors conducting penetration tests of agency systems are almost always successful in gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purposes they had in mind.

- ***Application Software Development and Change Controls.*** Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Without them, individuals can surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage. In many of our audits, we find that (1) testing procedures are undisciplined and do not ensure that implemented software operates as intended, (2) implementation procedures do not ensure that only authorized software is used, and (3) access to software program libraries is inadequately controlled.

- ***Segregation of Duties.*** Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes. We commonly find that computer programmers and operators are authorized to perform a wide variety of duties, thus providing them the ability to independently

modify, circumvent, and disable system security features. Similarly, we have also identified problems related to transaction processing, where all users of a financial management system can independently perform all of the steps needed to initiate and complete a payment.

- ***System Software Controls.*** System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation, e.g., operating systems, system utilities, security software, and database management systems. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosures. Our reviews frequently identify systems with insufficiently restricted access that in turn makes it possible for knowledgeable individuals to disable or circumvent controls.

- ***Service Continuity Controls.*** Service continuity controls ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, accidental loss of files, or even a major disaster such as a fire. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. At many of the agencies we have reviewed, we have found that plans and procedures are incomplete because operations and supporting resources had not been fully analyzed to determine which were most critical and would need to be restored first. In addition, disaster recovery plans are often not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

Actions Agencies Can Take Immediately to Reduce Risks

Agencies can act immediately to address the weaknesses just described and thereby reduce the related risks. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. None of these actions alone will ensure good security. However, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay. Let me briefly describe each of the actions I have mentioned.

Raise Awareness

First, agency security managers can take steps to ensure that agency personnel at all levels understand the significance of their dependence on computer support and the related risks to mission-related operations. Better understanding risks allows senior executives to make more informed decisions regarding appropriate levels of financial and personnel resources to protect these assets over the long term. However, we have found that when senior managers do not understand such risks, they may not devote adequate resources to security or be willing to tolerate the inconvenience that may be associated with maintaining adequate controls. In addition, system users must understand the importance of complying with policies and controls and why these controls are important to the agency in meeting its mission-critical functions. Engendering such understanding and awareness requires a proactive approach from agency security experts and, most important, support from the agency head.

Ensure Policies and Controls Are Operating Effectively

Second, agencies should ensure that the policies and controls they have already implemented are operating as intended. Our audits often find that security is weak, not because agencies have no policies and controls, but because the policies and controls they have implemented are not operating effectively. In some cases, they were never implemented appropriately. In other cases, the policies and controls have not been maintained. For example, assigning users password-controlled accounts on a system can be an effective way to help ensure that only authorized individuals gain access to the system. However, this control is significantly diminished if individuals who have retired, resigned, or otherwise left the agency retain access because system administrators have neglected to delete their accounts. To ensure that policies and controls are operating as intended, agencies must take steps to examine or test key controls routinely and enforce compliance with policies.

Implement Software Patches

Third, agencies should ensure that known software vulnerabilities are reduced by promptly implementing software patches. Security weaknesses are frequently discovered in commercial software packages after the software has been sold and implemented. To remedy these problems, vendors issue software "patches" that users of the software can install. In addition, organizations such as Carnegie Mellon University's CERT Coordination Center[9] routinely issue alerts on software problems.

[9]Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

However, our audits have found that such patches are often not installed promptly or not installed at all, thereby leaving serious and widely known vulnerabilities open to exploitation. To avoid this situation, agencies must establish procedures for routinely (1) keeping system administrators aware of the latest software vulnerability alerts and the related remedial actions that need to be taken and (2) ensuring that needed patches are implemented promptly.

Routinely Use Automated Tools to Monitor Security

Fourth, agencies can use readily available software tools to help ensure that controls are operating as intended and that their systems are secure. Examples of such tools are (1) scanners that automatically search for system vulnerabilities, (2) password cracking tools, which test password strength, and (3) network monitoring tools, which can be used to monitor system configurations and network traffic, help identify unauthorized changes, and identify unusual or suspicious network activity. Such tools provide an efficient way to monitor system security, and their use is increasingly viewed as an essential aspect of good security practice, especially when they are used as part of a comprehensive security self-assessment program. However, tool use must be carefully managed to ensure that tools are not misused and that they lead to meaningful improvement. If not properly managed, using them could slow system performance. Similarly, results must be carefully analyzed to determine which identified problems are the most significant and whether and how they can be remedied. Placing tool selection, use, and related training under the control of a central security group can help ensure that tools are used appropriately and effectively throughout the agency. Central analysis of scanning results can also facilitate identification of appropriate safeguards and assist the agency in better understanding its risks.

Identify and Propagate Pockets of Excellence

Fifth, agencies can expand on the good practices that they already have in place. Our audits have shown that even agencies with poor security programs often have good practices in certain areas of their security programs or certain organizational units. In these cases, we recommend that the agency expand or build on the practice throughout the agency. For example, one unit in one agency we recently audited had developed strong intrusion detection capabilities, but this capability was not being developed in other units of the agency. Once again, central coordination can help identify these pockets of excellence and ensure that their value is maximized on an agencywide basis.

Focus on the Most Common Vulnerabilities First

Finally, agencies can develop and distribute lists of the most common types of vulnerabilities, accompanied by suggested corrective actions, so that individual organizational units can take advantage of experience gained by others. Such lists can be developed based on in-house experience, or agencies can adapt lists available through professional organizations and other centers of expertise. In the course of our audits, we frequently find the same vulnerabilities over and over again. By encouraging managers to monitor for the most common vulnerabilities continually, agencies can help ensure that they area promptly addressed, thereby quickly reducing their risk and possibly freeing technical experts to identify and address more difficult problems.

Improved Security Program Management Is Essential

While the actions I have just outlined can jump-start agency security improvement efforts, they will not result in fully effective and lasting improvements unless they are supported by a strong management framework. Such a framework can ensure that

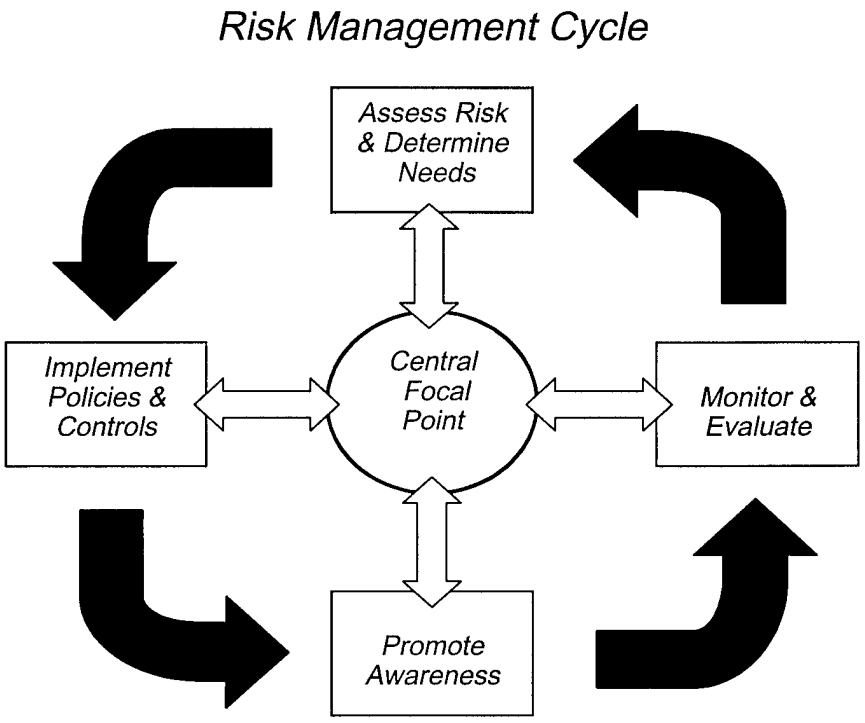
- agency actions are appropriately controlled and coordinated,
- testing tools are appropriately selected and tested prior to their use,
- personnel involved in using tools and in implementing software patches are properly trained,
- good practices and lessons learned are shared on an agencywide basis,
- controls are systematically tested to ensure that they are effective, and
- appropriate risk management decisions are made regarding the best way to address identified problems.

Establishing such a management framework requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,

- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments. This cycle of risk management activities is depicted below.



This cycle of activity, as described in our May 1998 executive guide, is consistent with guidance on information security program management provided to agencies by the Office of Management and Budget (OMB) and by the National Institute of Standards and Technology (NIST). In addition, the guide has been endorsed by the federal Chief Information Officers (CIO) Council as a useful resource for agency managers. We believe that implementing such a cycle of activity is the key to ensuring that information security risks are adequately considered and addressed on an ongoing basis.

Need for New Governmentwide Actions to Support Agency Security Efforts

While individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements could be strengthened. Existing requirements are somewhat out-of-date and do not provide agencies adequate guidance as to what levels of security are appropriate for their varying computer-supported operations. In addition, while the rigor and scope of our information security audits have increased in recent years, information on agency performance in this area is incomplete making it difficult to measure incremental improvements.

Perhaps most important, the legal framework supporting federal computer security needs to be updated. In particular, the Computer Security Act of 1987 is outmoded and inadequate, as well as poorly implemented. The act focuses too much attention on individual system security rather than requiring the agencywide perspective needed for today's networked environments. In addition, the act oversimplifies risk considerations by implying that there are only two categories of information: sensitive versus nonsensitive or classified versus nonqualified. As a result, it fails to recognize that security must be managed for a range of varying levels of risk to the integrity, availability, and confidentiality of information supporting agency operations and assets. Further, the act treats information security as a technical function rather than as a management function, which removes security from its integral role in program management. Lastly, the Computer Security Act does not require an evaluation of implemented controls (i.e., no testing). These deficiencies in the current legal framework lead directly to three specific areas where we believe governmentwide improvements are needed.

First, there is a need for routine periodic independent audits to provide (1) a basis for measuring agency performance and (2) information for strengthened oversight. Except for security audits associated with financial statement audits, current information security reviews are performed on an ad hoc basis.

Second, agencies need more prescriptive guidance regarding the level of protection that is appropriate for their systems. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. OMB and NIST guidance is not detailed enough to ensure that agencies are making appropriate judgments in this area and that they are protecting the same types of data consistently throughout the federal community. More specific guidance could be developed in two parts:

- A set of data classifications that could be used by all federal agencies to categorize the criticality and sensitivity of the data they generate and maintain. These classifications could range from noncritical, publicly available information requiring a relatively low level of protection to highly sensitive and critical information that requires an extremely high level of protection. Intermediate classifications could cover a range of financial and other important and sensitive data that require significant protection but not at the very highest levels. It would be important for these data classifications to be clearly defined and accompanied by guidelines regarding the types of data that would fall into each classification.

- A set of minimum mandatory control requirements for each classification. Such control requirements could cover issues such as (1) the strength of system user authentication techniques (e.g., passwords, smart cards, and biometrics) for each classification, (2) appropriate types of cryptographic tools for each classification, and (3) the frequency and rigor of testing appropriate for each classification.

Third, there is a need for stronger central leadership and coordination of information security-related activities across government. Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including OMB, NIST, the General Services Administration, and the National Security Agency. Other organizations are also becoming involved through the administration's critical infrastructure protection initiative, including the Department of Justice and the Critical Infrastructure Assurance Office. The federal CIO Council is also supporting these efforts. While all of these organizations have made positive contributions, some roles and responsibilities are not clear and central coordination is lacking in certain key areas. In particular, information on vulnerabilities and related solutions is not being adequately shared among agencies and requirements related to handling and reporting security incidents are not clear.

In conclusion, I want to emphasize that while there are many valuable tools and practices that agencies can adopt, there is no "silver bullet" for information security. Ensuring effective and efficient progress in this area throughout the federal government will require concerted efforts by senior executives, program managers, and technical specialists. It will require cooperative efforts by executive agencies and by the central management agencies, such as OMB. Further, it will require sustained congressional oversight to ensure that improvements are realized.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Subcommittee members may have. For future contacts regarding this testimony, please contact me at (202) 512-6240.

(511710)

Ordering Information

Orders by Internet

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)