United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Wednesday,
October 6, 1999

CRITICAL INFRASTRUCTURE PROTECTION

Fundamental Improvements Needed to Assure Security of Federal Operations

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

GAO/T-AIMD-00-7

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the "cyber," or computer security aspects of critical infrastructure protection. Since the early 1990s, an explosion in computer interconnectivity, most notably growth in use of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of facilitating communications, business processes, and access to information. However, without proper safeguards, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support including telecommunications, power distribution, emergency services, law enforcement, national defense, and other government services.

Today, I will focus on federal agency performance in addressing computer security issues. Recent audits by GAO and agency inspectors general (IG) show that our government is not adequately protecting critical federal operations and assets from computer-based attacks. These audits show that 22 of the largest federal agencies have significant computer security weaknesses. Addressing this widespread and persistent problem requires significant management attention and action within individual agencies as well as increased coordination and oversight at the governmentwide level. I will now provide greater detail on these problems and discuss broader issues that need to be considered as a national strategy for critical infrastructure protection is being considered.

Weak Controls Place Federal Programs at Risk

GAO and IG reports issued over the last 5 years describe persistent computer security weaknesses that place federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption as well as fraud and inappropriate disclosures.[1] Our most recent analysis, of reports issued during fiscal year 1999, identified significant computer security weaknesses in 22 of the largest federal agencies.[2] These included weaknesses in (1) controls over access to sensitive systems and data, (2) controls over software development and changes, and (3) continuity of service plans. These types of weaknesses increase the risk that intruders or authorized users with malicious intentions could read, modify, delete, or otherwise damage information or disrupt operations for purposes, such as fraud, sabotage, or espionage. This body of audit evidence led us, in February 1997 and again in January 1999, to designate information security as a governmentwide high-risk area in reports to the Congress.[3]

Examples of these weaknesses and the risks they present include the following.

- In May 1999, we reported 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. Having obtained access, we could have disrupted NASA's ongoing command and control operations and stolen, modified, or destroyed system software and data.[4]

[1] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996), *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[2] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-01, October 1, 1999).

[3] *High Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1997) *and High Risk Series: An Update* (GAO/HR-99-1, January 1999).

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

- In August 1999, we reported that serious weaknesses in Department of Defense (DOD) 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. These weaknesses impair DOD's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems is properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud.[5]
- In July 1999, we reported that the Department of Agriculture's (USDA) National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent and/or detect unauthorized changes to payroll and other payment data or computer software. NFC develops and operates administrative and financial systems, including payroll/personnel, property management, and accounting systems for both the USDA and more than 60 other federal organizations. During fiscal year 1998, NFC processed more than $19 billion in payroll payments for more than 450,000 federal employees. NFC is also responsible for maintaining records for the world's largest 401(k)-type program, the federal Thrift Savings Program. This program, which is growing at about $1 billion per month, covers about 2.3 million employees and totaled more than $60 billion as of September 30, 1998.[6] The weaknesses we identified increased the risk that users could cause improper payments and that sensitive information could be misused, improperly disclosed, or destroyed.
- In October 1999, we reported that Department of Veterans Affairs (VA) systems continued to be vulnerable to unauthorized access.[7] VA operates the largest healthcare delivery system in the United States and reported spending more than $17 billion on medical care in fiscal year

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

[6] *USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-99-227, July 30, 1999).

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

1998. The department also processed more than 42 million benefit payments totaling about $22 billion in fiscal year 1998 and provided life insurance protection through more than 2.4 million policies that represented about $23 billion in coverage. In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for veterans and their family members. GAO, as well as the VA IG, continued to find serious problems that placed sensitive information at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. For example, at one VA insurance center, 265 users who had not been authorized access had the ability to read, write, and delete information related to insurance awards. Such unauthorized access could lead to improper insurance payments.

Poor Security Program Management Is the Fundamental Cause of Poor Computer Security

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. We reported on this problem in 1996 and, again, in 1998,[5] noting that agency managers are not ensuring, on an ongoing basis, that risks are identified and addressed and that controls are operating as intended. In many cases, senior agency officials have not recognized that computer-supported operations are integral to carrying out their missions and that they can no longer relegate the security of these operations solely to lower-level technical specialists. For these reasons, it is essential that this fundamental problem be addressed as part of an effective information technology management strategy, which will also serve to strengthen critical infrastructure protection.

Agencies have responded to scores of recommendations for improvement made by us and by agency inspectors general. However, similar weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agencywide and ongoing basis. Instead, there is a tendency to react to individual audit findings as they are reported, with little ongoing attention to the systemic causes of control weaknesses.

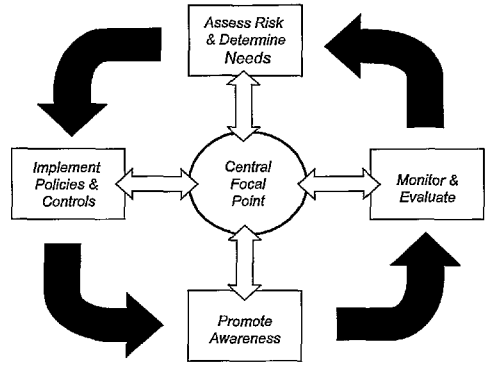
[5]GAO/AIMD-96-110, September 24, 1996, and GAO/AIMD-98-92, September 23, 1998.

To identify potential solutions to this problem, we studied the security management practices of eight nonfederal organizations known for their superior security programs. We found that these organizations managed their information security risks through a cycle of risk management activities.[9] The basic framework–built on 16 specific practices–allows risk management through an ongoing cycle of activities coordinated by a central focal point. The management process involves

- assessing risk to determine information security needs;
- developing and implementing policies and controls that meet these needs;
- promoting awareness to ensure that risks, roles, and responsibilities are understood; and
- instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

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

Figure 1: The Risk Management Cycle



The guide is generally consistent with OMB and NIST guidance on information security program management, and it has been endorsed by the Chief Information Officers (CIO) Council as a useful resource for agency managers.

One agency that has illustrated the value of these management practices in strengthening computer security is the Internal Revenue Service (IRS). IRS has made significant progress by acknowledging the seriousness of its computer security weaknesses, consolidating overall responsibility for computer security management, reevaluating its approach to computer security management, and developing a high-level plan for mitigating the identified weaknesses.[10]

[10] *IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk* (GAO/AIMD-99-38, December 14, 1998).

A Comprehensive Strategy for Improvement Is Needed

While adopting the practices recommended by the guide can better prepare agencies to protect their systems, detect attacks, and react to security breaches, other actions are also needed to improve oversight and otherwise address the problem from a governmentwide perspective.

Presidential Decision Directive (PDD) 63, issued in May 1998, recognized that addressing computer-based risks to our nation's critical infrastructures requires an approach that involves coordination and cooperation across federal agencies and among public and private-sector entities and other nations. In this regard, PDD 63 established several entities to coordinate infrastructure protection efforts.[11] However, the details of the PDD's approach have not been finalized. As a result, a major objective of PDD 63 to make the federal government "a model to the private sector on how best to protect critical infrastructure," has not been realized nor is it clear how this objective will be met.

To provide greater assurance that critical infrastructure objectives can be met, we believe that actions are needed in seven key areas. I will briefly discuss each of these.

Clearly Defined Roles and Responsibilities

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security; and the National Institute of Standards and Technology (NIST), with assistance from the National Security Agency (NSA), is responsible for establishing related standards.[12] In addition, interagency bodies, such as the CIO Council and the entities created under PDD 63 are attempting to coordinate agency initiatives.

While these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not taking place. This is due, in part, to the relative

[11]In May 1998, PDD 63 created several new entities in the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation which also have responsibility for guiding and overseeing and coordinating agency security with a focus on critical infrastructure protection.

[12]The Computer Security Act and the Paperwork Reduction Act.

immaturity of the recently established processes. It is also unclear how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Constraints on resources and the urgency of the problem require that government activities are designed and coordinated to achieve clearly understood goals. There must also be clear linkage between policy guidance, technical standards, and agency practices to ensure responsibility/accountability for actual improvements.

Specific Risk-Based Standards

Second, agencies need more specific guidance on the controls that they need to implement. Currently agencies have wide discretion in deciding (1) what computer security controls to implement and (2) the level of rigor with which they enforce these controls. In theory, this is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data.

However, our studies of best practices at leading organizations have shown that more specific guidance is important. In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; and help ensure that shared data are appropriately protected. Implementing such standards for federal agencies would require developing (1) a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain and (2) minimum mandatory requirements for protecting information in each classification category.

Routine Evaluations of Agency Performance

Third, routine periodic audits must be implemented to allow for meaningful performance measurement. A requirement for periodic examinations of controls in operation would significantly strengthen oversight requirements in the Computer Security Act, which focus on evaluating agency security plans, rather than practices.

Ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls

are operating as intended. Evaluations at several levels can be beneficial. Tests initiated by agency officials are essential because they provide information needed to fulfill their ongoing responsibility for managing security programs. Evaluations initiated by independent auditors, such as agency inspectors general, can serve as an independent check on management evaluations and provide useful information for congressional and executive branch oversight. Summary evaluations performed by entities such as OMB, GAO, or the CIO Council can provide a governmentwide view of progress and help identify crosscutting problems.

At present, there is no requirement for periodic independently initiated tests and evaluations of agency computer security programs. As a result, information for measuring the effectiveness of agency security programs, and thus, holding agency managers accountable is limited. While some control testing is done in support of annual independent financial statement audits, ensuring routine periodic testing of all critical agency systems–both financial and nonfinancial–may require new legislation.

Executive Branch and Congressional Oversight

Fourth, the executive branch and the Congress must effectively use audit results and performance measures to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential to hold agencies accountable for their performance and was demonstrated by the recent OMB and congressional efforts to oversee the Year 2000 challenge.

Adequate Technical Expertise

Fifth, it is important for agencies to have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. The Computer Security Act authorized NIST to provide assistance to agencies and included provisions for periodic training in computer security awareness and practice. However, as the Year 2000 challenge showed, the availability of adequate technical expertise has been a continuing concern to agencies.

A number of programs and recommendations have been proposed that merit congressional study. For example, prompted in part by concerns over technical staff shortages affecting Year 2000 efforts, the CIO Council's Education and Training committee studied ways to help agencies recruit and retain information technology personnel. The resulting report provides an extensive description of the current status of federal information

technology employment, improvement efforts currently underway, and detailed proposals for action.

Adequate Funding

Sixth, agencies must have resources sufficient to support their computer security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. Also, addressing the Year 2000 challenge has resulted in postponement of many program and information technology initiatives–including system enhancements and computer security.[13] OMB and congressional oversight of future spending on computer security will be important to ensure that agencies are not using the funds they receive to continue ad hoc, piece-meal security fixes not supported by a strong agency risk management framework.

Incident Response and Coordination

Seventh, there is a need to more comprehensively monitor and develop responses to intrusions, viruses, and other incidents that threaten federal systems. Several entities are already providing some central coordination in this area–including the FBI, NIST, and the FedCIRC.[14] However, the specific roles and responsibilities of these organizations, as well as the balance between governmentwide and individual agency responsibilities, should be clarified and expanded to provide a more comprehensive picture of the security events that are occurring and assistance in dealing with them.

Such efforts can take several forms that provide differing benefits. For example, a governmentwide response center could provide immediate emergency assistance to agencies experiencing intrusions or other potential problems. It could also provide assistance on a nonemergency basis, especially by alerting agencies to new threats and vulnerabilities and helping them identify actions to prevent or mitigate incidents. By calling on a center for such assistance, agencies could tap into a source of specialized

[13] *Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications* (GAO/T-AIMD-99-214, June 22, 1999).

[14] FedCIRC–the Federal Computer Incident Response Capability–is a reporting center at the General Services Administration.

expertise that may be difficult and expensive to maintain at the individual agency level. A governmentwide center could also serve as clearinghouse of information on incidents that would be available to federal agencies and the public. Such information can be valuable in estimating the significance of different types of information security risks. For example, when the Melissa virus surfaced earlier this year, we found that there was no single place to obtain complete data on what agencies were hit and how they were affected. Moreover, there were no data available that quantified the impact of the virus in terms of productivity lost or the value of data lost.

Finally, it is important to recognize that, by itself, a central clearinghouse is not complete solution for the information security problems across the federal government. Agencies themselves must still use this information effectively to assess risks to their own computer-supported operations and to develop and implement sound management controls.

In conclusion, Mr. Chairman, I want to stress that there are no simple solutions to improving computer security throughout the government. What is clear is that a bottom-up approach will not work. To begin to meet the lofty goal of PDD 63–making the government a model–will require sustained top management support, consistent oversight, and additional levels of technical and funding support. Taking steps to address the issues outlined in my statement could help the government put its own house in order and more effectively work with the private sector to protect critical infrastructures. This concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

Document No. 175