United States General Accounting Office

GAO

Testimony

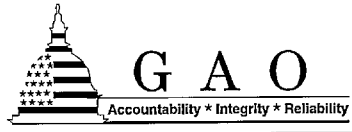
Before the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
1:30 p.m.
Thursday,
September 30, 1999

INFORMATION SECURITY

The Proposed Computer Security Enhancement Act of 1999

Statement of Keith A. Rhodes
Director, Office of Computer and Information Technology Assessment
Accounting and Information Management Division



GAO/T-AIMD-99-302

Madam Chairwoman and Members of the Subcommittee:

Thank you for asking me to participate in today's hearing on the proposed Computer Security Enhancement Act of 1999 (H.R. 2413). The legislation seeks to address the dramatic advances in information technology that have occurred since the Computer Security Act of 1987[1]–advances that have significantly increased risks to our computer systems and, more importantly, to the critical operations and infrastructures they support. In particular, H.R. 2413 aims to reinforce the role of the National Institute of Standards and Technology (NIST), whose mission is to provide guidance and technical assistance to government and industry to protect unclassified information systems.

Today, I would like to discuss (1) the urgent need to strengthen computer security across the federal government, (2) the current and future privacy concerns with any computer security legislation, (3) our views on the proposed act, and (4) what can be done to further strengthen security program management at individual agencies as well as governmentwide leadership, coordination, and oversight.

The Urgent Need to Strengthen Computer Security for the Federal Government

As hearings by this Subcommittee have recently emphasized, risks to the security of our government's computer systems are significant, and they are growing. The dramatic increase of computer interconnectivity and the popularity of the Internet, while facilitating access to information, are factors that also make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are readily available.

Attacks on and misuse of federal computer and telecommunications resources are of increasing concern because these resources are virtually indispensable for carrying out critical operations and protecting sensitive data and assets. For example, system break-ins at the Department of the

[1]The primary objectives of this act were to provide for (1) a computer standards program within the National Institute of Standards and Technology, (2) security and privacy for information in federal computer systems not covered by national security restrictions, and (3) training in security matters for persons involved in the management, operation, and use of federal computer systems.

Treasury could place billions of dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure. At the Department of Defense, operations such as mobilizing reservists, paying soldiers, and managing supplies could be affected as well as warfighting capability. At the Health Care Financing Administration, billions of dollars of claim payments and sensitive medical information could be affected.

Over the past year, this Subcommittee has focused[2] on a series of break-ins of federal web sites and the "Melissa" computer virus.[3] While these incidents resulted in relatively limited damage, they demonstrated the formidable challenge that the federal government faces in protecting its information systems assets and sensitive data. For example, Melissa and other recent viruses, such as "Explore Zip,"[4] showed just how quickly attacks can proliferate due to the intricate and extensive connectivity of today's networks–in just days after the virus was unleashed, there were widespread reports of "infections" throughout the country. They also demonstrated that vulnerabilities in commercial-off-the-shelf (COTS) products, which federal agencies are increasingly relying on to support critical federal operations, can be easily exploited to attack all their users.

Because of the increasing reliance on the Internet and standard COTS products, as well as the increasing improvements in computer attack tools and techniques (as evidenced in the additional capability and techniques deployed in the recent virus attacks), it is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and counter. Yet audits reports issued by us and agency inspectors general since 1996 have found that many agencies are not prepared to protect themselves from these evolving threats.

[2] *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999), *Information Security: Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management* (GAO/T-AIMD-99-223, June 24, 1999), and *Information Security: Answers to Posthearing Questions* (GAO/AIMD-99-272R, August 9, 1999).

[3] Melissa was a "macro virus" that could affect users of Microsoft's Word 97 or Word 2000 word processing software. Macro viruses are computer viruses that use an application's own macro programming language to reproduce themselves. The viruses can inflict damage to the document or to other computer software.

[4] ExploreZip was a virus designed to destroy electronic files, degrade network performance, and eventually cause a denial of service on electronic mail servers.

It is imperative, therefore, that the federal government swiftly implement long-term solutions both at individual agencies and governmentwide to protect systems and sensitive data. As I will further discuss today, these include strengthening security management by individual agencies, clarifying the roles of various federal organizations with responsibilities related to information security, identifying and ranking the most significant information security issues facing federal agencies, ensuring the adequacy of information technology workforce skills, periodically evaluating and testing agency information security practices, and assuring high-level executive branch leadership.

In recent years, NIST has had a valuable role in helping agencies to protect unclassified information systems and addressing advances in security technology. Since enactment of the Computer Security Act of 1987, NIST has had the responsibility for setting computer security standards for all federal agency systems except national security systems. National security system standards are set by the National Security Agency. NIST has also undertaken efforts to raise awareness of information technology vulnerabilities and protection requirements, facilitate the development of new technologies to provide system and network protection, and develop guidance to ensure effective security planning and management.

Computer Security Legislation and Privacy Concerns

Developing and implementing information security legislation can be a delicate balancing act. The need to protect sensitive data and systems must be weighed not only against cost and feasibility concerns but also the privacy and security interests of individual citizens and private businesses as well as national security and law enforcement agencies. However, without computer security, privacy cannot be assured.

For individuals and the private sector, the Internet is rapidly becoming an increasingly popular avenue of doing business. A study jointly sponsored by the University of Texas Center for Research in Electronic Commerce and Cisco Systems, Inc.[5] found that the Internet economy generated more than $300 billion in U.S. revenue and was responsible for 1.2 million jobs in 1998. The study also found that Internet commerce is growing at a much faster rate than expected–in 1998, total electronic commerce exceeded $102 billion for U.S.-based companies. Not surprisingly, security and

[5]See *www.internetindicators.com* for details on this study's findings.

privacy concerns have increased along with the popularity of electronic commerce. Customers are primarily concerned with credit card fraud, which has increased considerably over the past several years. Businesses are interested in protecting customers as well as their own information assets from competitors, vandals, criminals, suppliers, and foreign governments.

An important part of the solution to these security concerns is cryptography. Information that has been properly authenticated and encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic key. While information vulnerabilities cannot be eliminated through the use of any single tool, cryptography can help businesses ensure the confidentiality and integrity of information in transit and storage and verify the asserted identity of individuals and computer systems.

However, national security and law enforcement concerns must be considered as cryptographic tools become increasingly available. For example, encryption can prevent law enforcement authorities from gaining access to information needed to investigate and prosecute criminal activity. It can also threaten intelligence gathering for national security purposes.

At the same time, the use of encryption by the private sector can benefit law enforcement and national security interests. According to the National Research Council, by protecting the trade secrets and proprietary information of businesses, encryption can reduce economic espionage and thus support the job of law enforcement. By helping protect nationally critical information systems and networks (e.g., banking, telecommunications, and electric power) against unauthorized penetration, encryption can support the national security of the United States.[6]

Not only does this complex web of interests make it difficult to draft effective security legislation, it also makes it challenging to develop cryptographic and other security technology. Without obtaining agreement among individual users and businesses and law enforcement, national security, and other authorities on requirements, there is no way to build and implement the new technology or to establish standards that will be universally accepted.

[6] *Cryptography's Role in Securing the Information Society*, National Research Council, May 1996.

The Computer Security Enhancement Act Takes Positive Steps Toward Addressing Dramatic Advances in Information Technology

The proposed Computer Security Enhancement Act of 1999 takes a number of steps to address the proliferation of networked systems and the corresponding need for better protection over sensitive data belonging to both government and the private sector. If effectively implemented, these provisions can have a positive impact in addressing information security problems identified in our audits.

The bill particularly focuses on the role NIST plays in assisting federal agencies to protect their systems and promote technology solutions to security protection based on private sector offerings. While this legislation provides an improved basis for protecting critical federal assets, it is important to recognize that there is no legislative substitute that could be put in place to provide the increased management attention and due diligence necessary to implement and ensure the effectiveness of information security controls. It is also important to ensure that NIST retain the ability to develop security standards for unclassified data and decide which industry standards are appropriate for federal agencies, and that agencies themselves consistently implement such standards.

I would now like to comment on a few provisions in the bill that focus on NIST's role in helping agencies to protect their systems and ensure that NIST will play a vital role in helping to pioneer new security technologies.

First, the bill requires NIST to provide guidance and assistance to federal agencies in the protection of interconnected systems and to coordinate federal response efforts related to unauthorized access to federal computer systems. We support this measure, as federal response efforts have been sporadic and uneven to date. However, it will be important to make sure that NIST has the capability and authority needed to carry out this function.

Second, the bill requires the Under Secretary of Commerce to establish a clearinghouse of information available to the public on information security threats. We support the establishment of a clearinghouse; however, to be effective, it will be important for the information provided by the clearinghouse to be complete and useful for analyses of widespread attacks. As you may recall, when the Melissa virus surfaced earlier this year, we found that there was no single place to obtain complete data on which 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. Also, it may be necessary to clarify requirements for reporting incidents. Because there are several

entities already providing information on information security threats–including the Federal Bureau of Investigation and the FedCIRC[7]– it may be unclear to many agencies where incidents should be reported. Finally, it is important to recognize that by itself, a clearinghouse is not a panacea to 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.

Third, the bill requires the National Research Council to conduct a study to assess the desirability of public key infrastructures (PKI) and the technologies required for the establishment of such key infrastructures. Public key cryptography uses two electronic keys: a public key and a private key. A PKI provides the means to bind keys to their owners and helps in the distribution of reliable public keys in large networks.[8] As the use of the Internet by federal agencies, businesses, and citizens continues to expand, it is important that the benefits as well as the vulnerabilities of PKI as well as implementation concerns be thoroughly examined. For instance, the widespread use of PKI technology can help increase the confidence of electronic transactions, but to be effective, PKI components need to interoperate regardless of the source of the equipment and software involved, and they also need to be adequately secured. NIST has already been working with industry and technical groups to advance PKI technology and to develop standards that provide a basis for interoperable components, and we support these efforts.

Fourth, the bill establishes a National Policy Panel for Digital Signatures for the purpose of exploring issues relevant to the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities. Again, with the explosive growth of the Internet, there is an increasing demand for confidentiality and integrity with electronic

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

[8]According to NIST, public and private keys are mathematically related but the private key cannot be determined from the public key. The public key can be known by anyone while the private key is kept secret by its owner. As long as there is a strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. Public keys may be bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associate public key and are issued by a reliable certification authority.

commerce transactions. This means that the receiver of an electronic commerce message must be assured that the message came from the actual sender, that no part of the message has been altered during transmission, and that the contents of the transaction have been kept confidential. NIST has already been working with industry to test digital signature technology and to develop new approaches. We also support these efforts as they will ensure that NIST is well-positioned to assist in electronic commerce standardization efforts.

The Need for a Broader Information Security Improvement Framework

As stated earlier, it is important to recognize that in the long term, a more comprehensive governmentwide strategy needs to emerge to ensure that critical federal assets and operations are protected from evolving security threats. This strategy needs to address two of the most fundamental deficiencies in federal computer security: (1) poor agency security program planning and management and (2) ineffective governmentwide oversight.

At the agency level, a number of factors have consistently contributed to poor federal information security, including insufficient awareness and understanding of risks, a shortage of staff with needed technical expertise, a lack of systems and security architectures to facilitate implementation and management of security controls, and various problems associated with the availability and use of specific technical controls and monitoring tools. A more important underlying problem, however, is the lack of security program management and oversight to ensure that risks are identified and addressed and that controls are working as intended.

In our September 1998 report[9] on the overall state of federal information security, we noted that of 17 agencies where security planning was reviewed, all had deficiencies. Many agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented programs for testing and evaluating the effectiveness of the controls they relied on.

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

Recently, for example, we reported[10] that penetration tests we conducted at one of the National Aeronautics and Space Administration's (NASA) 10 field centers showed that mission-critical systems responsible for command and control of spacecraft as well as the processing and distributing of scientific data returned from space were vulnerable to unauthorized access. A major contributing factor to our ability to penetrate these systems was that NASA was not effectively and consistently managing information technology security throughout the agency. Specifically, it was not effectively assessing risks to its systems, implementing security policies and controls, monitoring policy compliance or the effectiveness of controls, providing required computer security training, and centrally coordinating responses to security incidents. In commenting on our report, NASA concurred with our findings and is taking actions to implement our recommendations.

To help agencies implement the kind of management framework that is required to effectively respond to evolving security requirements, in May 1998, we issued an executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). It describes a framework for managing risks through an ongoing cycle of activities coordinated by a central focal point. The guide, which is based on the best practices of organizations noted for superior information security programs, has been endorsed by the Chief Information Officers (CIO) Council. By adopting the practices recommended by the guide, agencies can be better prepared to protect their systems, detect attacks, and react to security breaches.

With regard to governmentwide oversight, over the last several years, a number of efforts have been initiated to strengthen central oversight and coordination for information security. For example, the Security Committee established by the CIO Council has taken steps to promote security awareness, improve agency access to incident response services, and support agency improvement efforts. Also, Presidential Decision Directive 63, issued in May 1998, called for a range of actions intended to improve federal agency computer security programs, establish a partnership between the government and private sector, and improve our nation's ability to detect and respond to serious attacks. It created several new entities for developing and implementing a strategy for critical

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

infrastructure protection and it tasked federal agencies with developing critical infrastructure protection plans. Since then, a variety of activities have taken place, including development and review of individual agency protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links with the private sector.

However, a number of issues still need to be resolved. At present, for example, there is no mechanism, such as required independent audits, for routinely testing and evaluating the effectiveness of agency information security programs.[11] As a result, little useful information is routinely available for measuring the effectiveness of agency security programs and, thus, holding agency managers accountable and identifying and addressing the most serious problems. Also, the proliferation of organizations with overlapping oversight and assistance responsibilities is a source of potential confusion among agency personnel and may be an inefficient use of scarce technical resources. Exacerbating this problem is confusion over which information security standards and guidance are mandatory, rather than optional.

Thus, as we previously recommended in 1998,[12] to substantively improve protection over sensitive data and critical infrastructures, the Congress needs to consider stronger measures that would ensure that executive agencies are doing the following.

- Carrying out their responsibilities outlined in laws and regulations requiring them to protect their information resources.
- Clearly delineating the roles of the various federal organizations with responsibilities related to security.
- Identifying and ranking the most significant information security issues facing federal agencies.
- Promoting information security risk awareness among senior agency officials whose critical operations rely on automated systems.
- Strengthening information technology workforce skills.
- Evaluating the security of systems on a regular basis.

[11]Some independent testing of systems is done through agency annual financial statement audits.

[12]GAO/AIMD-98-92.

- Providing for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

Madam Chairwoman, this concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

Contacts and Acknowledgements

For information about this testimony, please contact Keith Rhodes at (202) 512-6415. Cristina Chaplain and Chris Martin made key contributions to this testimony.

Document No. 174