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.
Thursday,
June 22, 2000

CRITICAL INFRASTRUCTURE PROTECTION

Comments on the Proposed Cyber Security Information Act of 2000

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the proposed Cyber Security Information Act of 2000 (H.R. 4246), which is intended to remove barriers to information sharing between government and private industry in order to better address threats to the nation's critical infrastructure.

The concern over cyber threats is well placed. While the explosive growth in interconnectivity has contributed immeasurably to the nation's economy and well being, it also presents significant risks to our nation's computer systems and to the critical operations and infrastructures they support, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. Accordingly, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare. Nevertheless, because the federal government does not own all of our nation's critical infrastructures, it is limited in what it can do to protect these assets, and solutions must be tailored sector by sector, through partnerships with sector representatives that address threats, vulnerabilities, and possible response strategies.

Today, I will discuss how H.R. 4246 can enhance critical infrastructure protection and the formidable challenges involved with achieving the goals of the bill. In short, by removing key barriers that are precluding private industry from sharing information about infrastructure threats and vulnerabilities, H.R. 4246 can help build the meaningful private-public partnerships that are integral to protecting critical infrastructure assets. However, to successfully engage the private sector, the federal government itself must be a model of good information security. Currently, it is not. Significant computer security weaknesses–ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, to nonexistent or weak continuity of service plans–pervade virtually every major agency. And, as illustrated by the recent ILOVEYOU computer virus, mechanisms already in place to facilitate information sharing among federal agencies about impending threats and vulnerabilities have not been working effectively. Moreover, the federal government may not yet have the right tools for identifying, analyzing, coordinating, and disseminating the type of information that H.R. 4246 envisions collecting from the private sector.

Concerns About Risks to Our Critical Infrastructure Are Growing

Before discussing the specifics of H.R. 4246, I would like to provide an overview of the risks of severe disruption facing our nation's critical infrastructure and the steps being taking to address these risks. In particular, the explosive growth in computer interconnectivity over the past 10 years has significantly increased the risk that vulnerabilities exploited within one system will affect other connected systems. Massive computer networks now provide pathways among systems that if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as earthquakes, and system-induced problems, such as the Year 2000 (Y2K) date conversion problem, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

The resulting damage can vary, depending on the threat. Critical operations can be disrupted or otherwise sabotaged, sensitive data can be read and copied, and data or processes can be tampered with. A significant concern is that terrorists or hostile foreign states could launch computer-based attacks on critical systems, such as those supporting energy distribution, telecommunications, and financial services, to severely damage or disrupt our national defense or other operations, resulting in harm to the public welfare. Understanding these risks to our computer-based infrastructures and determining how best to mitigate them are major information security challenges.

The federal government is beginning to take steps to address those challenges. In 1996, the President's Commission on Critical Infrastructure Protection was established to investigate our nation's vulnerability to both cyber and physical threats. In its October 1997 report, *Critical Foundations: Protecting America's Infrastructures,* the Commission described the potential devastating implications of poor information security from a national perspective.

In May 1998, Presidential Decision Directive 63 (PDD 63) was issued in response to this report and recognized that addressing computer-based risks to our nation's critical infrastructures required a new approach that involves coordination and cooperation across federal agencies and among public- and private-sector entities and other nations. PDD 63 created several new entities for developing and implementing a strategy for critical infrastructure protection. In addition, it tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors. Since then, a variety of activities have been undertaken, including development and review of individual agency

critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links with the private sector.

In January 2000, the White House released its *National Plan for Information Systems Protection*[1] as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. This plan focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructures. Subsequent plans are to address a broader range of concerns, including the specific roles industry and state and local governments will play in protecting physical and cyber-based infrastructures from deliberate attacks as well as international aspects of critical infrastructure protection. The end goal of this process is to develop a comprehensive national strategy for critical infrastructure assurance, as envisioned by PDD 63, and to have this plan fully operational in 2003.

The plan proposes achieving its twin goals of making the U.S. government a model of information security and developing public-private partnerships to defend our national infrastructure through 10 programs listed in figure 1.

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue.* January 7, 2000. The White House.

Figure 1: Programs Identified in the National Plan for Information Systems Protection

- Identifying critical infrastructure assets and shared interdependencies
- Detecting attacks and unauthorized intrusions
- Developing intelligence and law enforcement capabilities to protect critical information systems
- Sharing attack warning and information in a timely manner
- Creating capabilities for response, reconstitution, and recovery
- Enhancing research and development
- Training and employing adequate numbers of information security specialists
- Conducting security awareness outreach efforts
- Adopting legislation and appropriations to support infrastructure protections
- Protecting privacy, civil liberties, and proprietary interests

The program involving sharing attack warning and information specifically seeks to bolster information exchange efforts with the private sector. In particular, the program aims to establish a Partnership for Critical Infrastructure Security and a National Infrastructure Assurance Council to increase corporate and government communications about shared threats to critical information systems. It also encourages the creation of Information Sharing and Analysis Centers (ISAC) to facilitate public-private sector information sharing about actual threats and vulnerabilities in individual infrastructure sectors. Two ISACs are already in operation: (1) the Financial Services ISAC, which exclusively serves the banking, securities, and insurance industries, and (2) the National Coordinating Center for Telecommunications, which is a joint industry/government organization. Several more ISACs are expected to be established by the end of the year.

H.R. 4246 and Its Potential Benefits for Critical Infrastructure Protection

Partnerships such as the ISACs are central to addressing critical infrastructure protection. However, some in the private sector have expressed concerns about voluntarily sharing information with the government. For example, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith.

H.R. 4246 was introduced on April 12, 2000, with the aim of addressing these concerns and encouraging the secure disclosure and exchange of information about cyber security problems and solutions. In many respects, the bill is modeled after the Year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector in order to facilitate the sharing on information on Y2K readiness. In particular, H.R. 4246:

- protects information being provided by the private sector from disclosure by federal entities under FOIA or disclosure to or by any third party,
- prohibits the use of the information by any federal and state organization or any third party in any civil actions, and
- enables the President to establish and terminate working groups composed of federal employees for the purposes of engaging outside organizations in discuss to address and share information about cyber security.

In essence, the bill seeks to enable the federal government to ask industry questions about events or incidents threatening critical infrastructures, correlate them at a national level in order to build a baseline understanding of infrastructures, and use these baselines to identify anomalies and attacks—something it is not doing now.

Addressing similar concerns proved valuable in addressing the Y2K problem. Although Y2K was a unique and finite challenge, it parallels the critical infrastructure challenge in some important respects. Like critical infrastructure protection, for instance, Y2K spanned the entire spectrum of our national, as well as the global, economy. Moreover, given the scores of interdependencies among private sector companies, state and local governments, and the federal government, a single failure in one system could have repercussions on an array of public and private enterprises. As a result, public/private information sharing was absolutely essential to ensuring compliance in supply chain relationships and reducing the amount of Y2K work.

Early on, Y2K information bottlenecks were widespread in the private sector. According to the President's Council on Year 2000 Conversion,[2] antitrust issues and a natural tendency to compete for advantage made working together on Y2K difficult, if not inconceivable, for many companies. Moreover, the threat of lawsuits had companies worried that they would be held liable for anything they said about the Y2K compliance of products or devices they used or test processes and results for them. Legal considerations also prevented companies from saying anything about their own readiness for date change. Thus, as noted by the council, their business partners, as well as the general public, may have assumed the worst.

According to the council, the Year 2000 Information and Readiness Disclosure Act paved the way for more disclosures about Y2K readiness and experiences with individual products and fixes. Several major telecommunications companies, for example, indicated their willingness to share Y2K information with smaller companies who contacted them. And the leaders of the electric power industry began a series of regional conferences for local distribution companies in which they discussed identified problems and solutions, particularly with embedded chips, as well as testing protocols and contingency planning.

Moreover, the act helped facilitate the work of the more than 25 sector-based working groups established by the council and other outreach activities. For example, the council and federal agencies were able to establish partnerships with several private-sector organizations, such as the North American Electric Reliability Council, to gather information critical to the nation's Y2K efforts and to address issues such as contingency planning. Concerned about the lack of information in some key industry areas, the council also convened a series of roundtable meetings in the spring and summer of 1999, which helped to shed light on the status of readiness efforts relating to pharmaceuticals, food, hospital supplies, transit, public safety, the Internet, education, and chemicals. The assessment reports resulting from these and other activities substantially increased the nation's understanding of the Y2K readiness of key industries.

Removing barriers to information sharing between government and industry can similarly enhance critical infrastructure protection. Both government and industry are key components of the infrastructure, both are potential targets for cyber threats, and both face significant gaps in

[2] *The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion,* March 29, 2000.

effectively dealing with the threats. As such, both must work together to identify threats and vulnerabilities and to develop response strategies. In particular, by combining information concerning the type of incidents and attacks experienced with the information obtained through federal intelligence and law enforcement sources, the government can develop and share more informative warnings and advisories. In turn, companies can develop a better understanding of the threats facing their particular infrastructures and be better prepared to take appropriate actions to protect their sectors.

Challenges in Building Public/Private Partnerships

By addressing private sector concerns about sharing information, H.R. 4246 could have a positive effect similar to the one the Year 2000 Information and Readiness Disclosure Act had in resolving the Y2K problem. At the same time, there are two formidable challenges to making this legislation a success.

First, while information sharing is important, the government needs to be sure that it is collecting the right type of information, that it can effectively synthesize and analyze it, and that it can appropriately share its analysis. A significant amount of work still needs to be done just in terms of ensuring that the right type of information is collected. For example, what information is required that will enable the government to detect a nationally significant cyber attack? Will information on intrusions, software anomalies, or reports of significant system failures provide an accurate baseline for making these determinations? Today, officials in the intelligence community do not know with real certainty what constitutes a cyber attack. Further, a 1996 Defense Science Board report stressed that understanding the information warfare process and indications of information warfare attacks will likely require an unprecedented effort to collect, consolidate, and synthesize data from a range of owners of infrastructure assets. The ISACs being established to facilitate public-private sector information sharing can assist in meeting this challenge. However, as noted earlier, only two ISACS are in operation and proposals regarding these centers are presented only in broad terms in the administration's preliminary National Plan for Information Systems Protection.

Once the government is sure that it is asking for the right type of information, it will need effective mechanisms for collecting and analyzing it. Building a common operational picture of critical infrastructures and determining if an attack is underway requires the government to develop capabilities to quickly and accurately correlate information from different infrastructures and reports of security incidents. This is a complex and

challenging task in itself. Data on possible threats—ranging from viruses, to hoaxes, to random threats, to news events, and computer intrusions—must be continually collected and analyzed from a wide spectrum of globally distributed sources in addition to sector-based groups. Nevertheless, fusing the right information from the public and private sectors in an operational setting is essential to detecting, warning, and responding to information-based attacks.

The National Infrastructure Protection Center (NIPC), located in the Federal Bureau of Investigation, is charged with this mission, but it is not clear whether NIPC has the right tools and resources needed to successfully coordinate information collection efforts with the private sector and to effectively correlate and analyze information received. We are currently engaged in an effort to review this capability.

In addition to collecting and analyzing data, the federal government needs to be able to effectively share information about infrastructure threats. Again, NIPC is charged with this responsibility and we are also reviewing its capability with respect to this issue. But, already, results in this area have been mixed. In December 1999, NIPC provided early warnings about a rash of denial-of-service attacks prominently on its website—2 months before the attack arrived in full force–and offered a tool that could be downloaded to scan for the presence of the denial of service code.

However, as we recently testified,[3] NIPC had less success with the ILOVEYOU virus. NIPC first learned of the virus at 5:45 a.m. EDT from an industry source, yet it did not issue an alert about the virus on its own web page until 11 a.m.—hours after many federal agencies were reportedly hit. This notice was a brief advisory; NIPC did not offer advice on dealing with the virus until 10 p.m. that evening. The lack of a more effective early warning clearly affected most federal agencies. Only 7 of 20 we contacted were spared widespread infection, which resulted in slowing some agency operations and requiring the diversion of technical staff toward stemming the virus' spread and cleaning "infected" computers. Moreover, NIPC did not directly warn the financial services ISAC about the impending threat.

The second challenge to realizing the goals of H.R. 4246 is that, to truly engage the private sector, the federal government needs to be a model for computer security. Currently, the federal government is not a model. As

[3] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000) and *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000).

emphasized in the National Plan for Information Systems Protection, the federal government specifically needs to be able to demonstrate that it can protect its own critical assets from cyber attack as well as lead research and development and educational efforts in the field of computer security. However, audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, to nonexistent or weak continuity of service plans.[4]

Importantly, our audits have repeatedly identified serious deficiencies in the most basic controls over access to federal systems. For example, managers often provided overly broad access privileges to very large groups of users, affording far more individuals than necessary the ability to browse, and sometimes modify or delete, sensitive or critical information. In addition, access was often not appropriately authorized or documented; users often shared accounts and passwords or posted passwords in plain view; software access controls were improperly implemented; and user activity was not adequately monitored to deter and identify inappropriate actions.

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. Agencies have not established the basic management framework needed to effectively protect their systems. Based on our 1998 study[5] of organizations with superior security programs, this involves managing information security risks through a cycle of risk management activities that include (1) assessing risk and determining protection needs, (2) selecting and implementing cost-effective policies and controls to meet these needs, (3) promoting awareness of policies and controls and of the risks that prompted their adoption, and (4) implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls. Additionally, a strong central focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

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

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

I would also like to emphasize that 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 also need to be strengthened. Specifically, there is a need for routine periodic independent audits of agency security programs to provide a basis for measuring agency performance and information for strengthened oversight. As we recently testified,[6] a bill has been introduced in the Senate this year—the Proposed Government Information Security Act (S. 1993)—which provides a requirement for such audits. There is also a need for

- more prescriptive guidance regarding the level of protection that is appropriate for their systems,
- strengthened central leadership and coordination of information security-related activities across government,
- strengthened incident detection and response capabilities, and
- adequate technical expertise and funding.

For example, central leadership and coordination of information security-related activities across government is lacking. Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including

- the Office of Management and Budget (OMB), which is responsible for developing information security policies and overseeing agency practices;
- the National Institute of Standards and Technology, which is charged with developing technical standards and providing related guidance for sensitive data; and
- the National Security Agency, which is responsible for setting information security standards for national security agencies.

Other organizations are also becoming involved through the administration's critical infrastructure protection initiative, including NIPC; the Critical Infrastructure Assurance Office, which is working to foster private-public relationships; and the Federal Computer Incident

[6] *Information Security: Comments on the Proposed Government Information Security Act of 1999,* (GAO/T-AIMD-00-107, March 2, 2000).

Response Capability (FedCIRC), which is the central coordination and analysis facility dealing with computer security–related issues affecting the civilian agencies and departments across the federal government. While some coordination is occurring, overall, this has resulted in a proliferation of organizations with overlapping oversight and assistance responsibilities. Absent is a strong voice of leadership and a clear understanding of roles and responsibilities.

As we recently testified,[7] having strong, centralized leadership has been critical to addressing other governmentwide management challenges. For example, vigorous support from officials at the highest levels of government was necessary to prompt attention and action to resolving the Y2K problem. Similarly, forceful, centralized leadership was essential to pressing agencies to invest in and accomplish basic management reforms mandated by the Chief Financial Officers Act. To achieve similar results for critical infrastructure protection, the federal government must have the support of top leaders and more clearly defined roles for those organizations that support governmentwide initiatives.

In summary, by removing private sector concerns about sharing information on critical infrastructure threats, H.R. 4246 can facilitate private-public partnerships and help spark the dialogue needed to identify threats and vulnerabilities and to develop response strategies. For the concepts in H.R. 4246 to work, however, this legislation needs to be accompanied by aggressive outreach efforts; effective centralized leadership; and good tools for collecting, analyzing, and sharing information. Moreover, the federal government cannot realistically expect to engage private-sector participation without putting its own house in order. Doing so will require concerted efforts by senior executives, program managers, and technical specialists to institute the basic management framework needed to effectively detect, protect against, and recover from critical infrastructure attacks. Moreover, it will require cooperative efforts by executive agencies and by the central management agencies, such as OMB, to address crosscutting issues and to ensure that improvements are realized.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

[7] *Information Security: Comments on the Proposed Government Information Security Act of 1999* (GAO/T-AIMD-00-107, March 2, 2000).

Contacts and Acknowledgments

For questions regarding this testimony, please contact Jack L. Brock, Jr. at (202) 512-6240. Individuals making key contributions included Cristina Chaplain, Michael Gilmore, and Paul Nicholas.

(512009)

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)