United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on

For Release on Delivery
Expected at 10:00 a.m.
EDT
Wednesday, March 16,
2011

CYBERSECURITY

Continued Attention Needed to Protect Our Nation’s Critical Infrastructure and Federal Information Systems

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

GAO
Accountability * Integrity * Reliability

Chairman Lungren, Ranking Member Clarke, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the cyber threats to critical infrastructure and the American economy.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal and nonfederal systems and operations. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[1] Recent press reports that computer hackers broke into and stole proprietary information worth millions of dollars from the networks of six U.S. and European energy companies also demonstrate the risk that our nation faces. Such attacks highlight the importance of developing a concerted response to safeguard federal and nonfederal information systems.

Mr. Chairman, GAO recently issued its high-risk list of government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. [2] Once again, we identified protecting the federal government's information systems and the nation's

[1] Director of National Intelligence, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community*, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

[2] GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

cyber critical infrastructure as a governmentwide high-risk area. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation’s critical infrastructure, referred to as cyber critical infrastructure protection or cyber CIP.

In my testimony today I will describe (1) cyber threats to cyber-reliant critical infrastructures and federal information systems and (2) the continuing challenges federal agencies face in protecting the nation’s cyber-reliant critical infrastructures and federal systems. In preparing this statement in March 2011, we relied on our previous work in these areas (please see the related GAO products page at the end of this statement). These products contain detailed overviews of the scope and methodology we used. The work on which this statement is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies and our nation’s critical infrastructures[3]— such as power distribution, water supply, telecommunications, and emergency services —have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transfer increasing amounts of money and sensitive and proprietary information, conduct operations, and deliver services to constituents.

The security of these systems and data is essential to protecting national and economic security, and public health and safety. Conversely, ineffective information security controls can result in significant risks, including the loss of resources, such as federal payments and collections; inappropriate access to sensitive information, such as national security information, personal information on taxpayers, or proprietary business information; disruption of critical operations supporting critical infrastructure, national defense, or emergency services; and undermining of agency missions due to embarrassing incidents that diminish public confidence in government.

Cyber-reliant Critical Infrastructure and Federal Systems Face Increasing Cyber Threats

Threats to systems supporting critical infrastructure and federal information systems

[3] Critical infrastructures are systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

are evolving and growing. Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and foreign nations. Federal law enforcement and intelligence agencies have identified multiple sources of threats to our nation’s critical information systems, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors. These groups and individuals have a variety of attack techniques at their disposal that can be used to determine vulnerabilities and gain entry into targeted systems. For example, *phishing* involves the creation and use of fake e-mails and Web sites to deceive Internet users into disclosing their personal data and other sensitive information.

The connectivity between information systems, the Internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. For example, in May 2008, we reported that the Tennessee Valley Authority’s (TVA) corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[4] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA’s critical infrastructures and 73 recommendations to address weaknesses in information security controls. TVA concurred with

[4] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

the recommendations and has taken steps to implement them. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about U.S. citizens has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. Further, reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating.

When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). Over the past 5 years, the number of incidents reported by federal agencies to US-CERT has increased dramatically, from 5,503 incidents reported in fiscal year 2006 to about 41,776 incidents in fiscal year 2010 (a more than 650 percent increase). The three most prevalent types of incidents and events reported to US-CERT during fiscal year 2010 were: (1) malicious code (software that infects an operating system or application), (2) improper usage (a violation of acceptable computing use policies), and (3) unauthorized access (where an individual gains logical or physical access to a system without permission). Additionally, according to Department of Homeland Security (DHS) officials, US-CERT detects incidents and events through its intrusion detection system, supplemented by agency reports, for investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

Reports of cyber attacks and information security incidents against federal systems and systems supporting critical infrastructure illustrate the effect that such incidents could have on national and economic security.

- In July 2010, the Department of Defense (DOD) launched an investigation to identify how thousands of classified military documents (including Afghanistan and Iraq war operations, as well as field reports on Pakistan) were obtained by the group WikiLeaks.org. According to DOD, this investigation was related to an ongoing investigation of an Army private charged with, among other things, transmitting national defense information to an unauthorized source.

- In 2010, the Deputy Secretary of Defense stated that DOD suffered a significant compromise of its classified military computer networks in 2008. It began when a flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network and spread on both classified and unclassified systems.[5]

- In February 2011, media reports stated that computer hackers broke into and stole proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.

The Federal Government Has Taken Actions to Address Cyber Threats, but Challenges Remain in Protecting Critical Systems

The federal government has a variety of roles and responsibilities in protecting the nation’s cyber-reliant critical infrastructure, enhancing the nation’s overall cybersecurity posture, and ensuring the security of federal systems and the information they contain. In light of the pervasive and increasing threats to critical systems, the executive branch is taking a number of steps to strengthen the nation’s approach to cybersecurity. For example, in its role as the focal point for federal efforts to protect the nation's cyber critical infrastructures,[6] DHS issued a revised national infrastructure protection plan in 2009 and an interim national cyber incident response plan in 2010. Executive branch agencies have also made progress instituting several governmentwide initiatives

[5] Foreign Affairs, *Defending a New Domain: The Pentagon’s Cyberstrategy*, William J. Lynn III, U.S. Deputy Secretary of Defense (New York, N.Y.: September/October 2010).

[6] As established by federal law and policy, including the Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

that are aimed at bolstering aspects of federal cybersecurity, such as reducing the number of federal access points to the Internet, establishing security configurations for desktop computers, and enhancing situational awareness of cyber events. Despite these efforts, the federal government continues to face significant challenges in protecting the nation’s cyber-reliant critical infrastructure and federal information systems.

Key Actions to Improve Our Current National Approach to Cybersecurity Have Not Yet Been Fully Implemented

The administration and executive branch agencies have not yet fully implemented key actions that are intended to address threats and improve the current U.S. approach to cybersecurity.

- *Implementing actions recommended by the president’s cybersecurity policy review.* In February 2009, the president initiated a review of the government’s cybersecurity policies and structures, which resulted in 24 near- and mid-term recommendations to address organizational and policy changes to improve the current U.S. approach to cybersecurity.[7] In October 2010, we reported that 2 recommendations had been implemented and 22 were partially implemented.[8] Officials from key agencies involved in these efforts (e.g. DHS, DOD, and the Office of Management and Budget (OMB)) stated that progress

[7] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[8] GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (Washington, D.C.: October 6, 2010).

had been slower than expected because agencies lacked assigned roles and responsibilities and because several of the mid-term recommendations would require action over multiple years. We recommended that the national Cybersecurity Coordinator (whose role was established as a result of the policy review) designate roles and responsibilities for each recommendation and develop milestones and plans, including measures to show agencies' progress and performance.

- *Updating the national strategy for securing the information and communications infrastructure.* In March 2009, we testified on the needed improvements to the nation's cybersecurity strategy.[9] In preparation for that testimony, we convened a panel of experts that included former federal officials, academics, and private sector executives. The panel highlighted 12 key improvements that are, in its view, essential to improving the strategy and our national cybersecurity posture, including the development of a national strategy that clearly articulates strategic objectives, goals, and priorities.

- *Developing a comprehensive national strategy for addressing global cybersecurity and governance*. In July 2010, we reported that the U.S. government faced a number of challenges in formulating and implementing a coherent approach to global aspects of cyberspace, including, among other things, providing top-level leadership and developing a comprehensive strategy.[10]

[9] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

[10] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

Specifically, we found that the national Cybersecurity Coordinator’s authority and capacity to effectively coordinate and forge a coherent national approach to cybersecurity were still under development. In addition, the U.S. government had not documented a clear vision of how the international efforts of federal entities, taken together, support overarching national goals. We recommended that, among other things, the national Cybersecurity Coordinator develop with other relevant entities a comprehensive U.S. global cyberspace strategy. The coordinator and his staff concurred with our recommendations and stated that actions had already been initiated to address them.

- *Finalizing cybersecurity guidelines and monitoring compliance related to electricity grid modernization*. In January 2011, we reported on efforts by the National Institute of Standards and Technology (NIST) to develop cybersecurity guidelines and Federal Energy Regulatory Commission (FERC) efforts to adopt and monitor cybersecurity standards related to the electric industry’s incorporation of IT systems to improve reliability and efficiency—commonly referred to as the smart grid.[11] We determined that NIST had not addressed all key elements of cybersecurity in its initial guidelines or finalized plans for doing so. We also determined that FERC had not developed an approach for monitoring industry compliance with its initial set of voluntary standards. Further, we identified six key challenges with respect to securing smart grid systems, including a lack of security features

[11] GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117 (Washington, D.C.: Jan. 12, 2011).

being built into certain smart grid systems and an ineffective mechanism for sharing information on cybersecurity within the industry. We recommended that NIST finalize its plans for updating its cybersecurity guidelines to incorporate missing elements and that FERC develop a coordinated approach to monitor voluntary standards and address any gaps in compliance. Both agencies agreed with these recommendations.

- *Creating a prioritized national and federal cybersecurity research and development (R&D) agenda.* In June 2010, we reported that while efforts to improve cybersecurity R&D are under way by the White House's Office Science and Technology Policy (OSTP) and other federal entities, six major challenges impeded these efforts.[12] Among the most critical was the lack of a prioritized national cybersecurity research and development agenda. We found that despite its legal responsibility and our past recommendations, a key OSTP subcommittee had not created a prioritized national R&D agenda, increasing the risk that research pursued by individual organizations will not reflect national priorities. We recommended that OSTP direct the subcommittee to take several actions, including developing a national cybersecurity R&D agenda. OSTP agreed with our recommendation and provided details on planned actions.

We are in the process of verifying actions taken to implement our recommendations. In addition, we have ongoing work related to cyber CIP efforts in

[12] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development*, GAO-10-466 (Washington, D.C.: June 3, 2010).

several other areas including (1) cybersecurity-related standards used by critical infrastructure sectors, (2) federal efforts to recruit, retain, train, and develop cybersecurity professionals, and (3) federal efforts to address risks to the information technology supply chain.

Federal Capacity to Protect Against Cyber Threats Needs to Improve

In addition to improving our national capability to address cybersecurity, executive branch agencies, in particular DHS, also need to improve their capacity to protect against cyber threats by, among other things, advancing cyber analysis and warning capabilities and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure.

- *Enhancing cyber analysis and warning capabilities*. In July 2008, we reported that DHS's US-CERT had not fully addressed 15 key attributes of cyber analysis and warning capabilities.[13] As a result, we recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations and has reported that it is taking steps to implement them. We are currently working with DHS officials to determine the status of their efforts to address these recommendations.

[13] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: Jul. 31, 2008).

- *Strengthening the public-private partnerships for securing cyber critical infrastructure.* In July 2010, we reported that the expectations of private sector stakeholders were not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.[14] Federal partners, such as DHS, were taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements. We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving private sector sharing of sensitive information. We recommended that the national Cybersecurity Coordinator and DHS work with their federal and private sector partners to enhance information-sharing efforts, including leveraging a central focal point for sharing information among the private sector, civilian government, law enforcement, the military, and the intelligence community. DHS officials stated that they have made progress in addressing these recommendations, and we will be determining the extent of that progress as part of our audit follow-up efforts.

Federal Agencies Have Not Addressed Persistent Control Weaknesses or Implemented Effective Information Security Programs

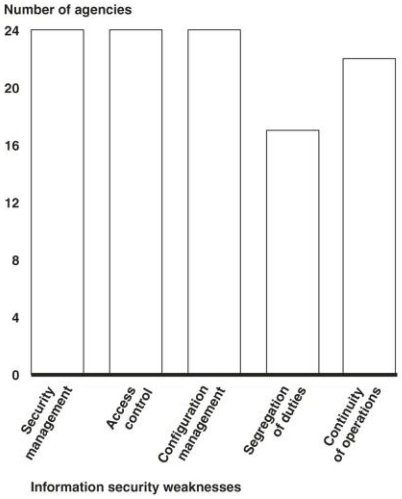
Federal systems continue to be afflicted by persistent information security control weaknesses. Specifically, agencies did not consistently implement effective controls to prevent, limit, and detect unauthorized access or

[14] GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628 (Washington, D.C.: July 15, 2010).

manage the configuration of network devices to prevent unauthorized access and ensure system integrity. Most of the 24 major federal agencies had information security weaknesses in five key internal control categories,[15] as illustrated in figure 1. In addition, GAO determined that serious and widespread information security control deficiencies were a governmentwide material weakness in internal control over financial reporting as part of its audit of the fiscal year 2010 financial statements for the United States government.

[15] The five internal controls are access controls, which ensure that only authorized individuals can read, alter, or delete data; configuration management controls, which provide assurance that only authorized software programs are implemented; segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and an agencywide information security program (security management), which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

Figure 1: Information Security Weaknesses at Major Federal Agencies for ~~Fiscal~~ FY~~Year~~ 2010



Source: GAO analysis of agency, inspector general, and GAO reports.

Over the past several years, we and inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

In addition, the White House, OMB, and selected federal agencies have undertaken governmentwide initiatives to enhance information security at federal agencies. For example, the Comprehensive National Cybersecurity Initiative, a series of 12 projects, is aimed primarily at improving DHS's and other federal agencies' efforts to reduce vulnerabilities, protect against intrusion attempts, and anticipate future threats against federal executive branch information systems. However, the projects face challenges in achieving their objectives related to securing federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. These challenges require sustained attention, which agencies have begun to provide.

In summary, the threats to information systems are evolving and growing, and systems supporting our nation's critical infrastructure and federal systems are not sufficiently protected to consistently thwart the threats. Administration and executive branch agencies need to take actions to improve our nation's cybersecurity posture, including implementing the actions recommended by the president's cybersecurity policy review and enhancing cyber analysis and warning capabilities. In addition, actions are needed to enhance security over federal systems and information, including fully developing and effectively implementing agencywide information security programs and implementing open recommendations. Until these actions are taken, our nation’s federal and nonfederal cyber critical infrastructure will remain vulnerable. Mr. Chairman, this completes my statement. I would be happy to answer any questions you or other Members of the Subcommittee have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Michael Gilmore (Assistant Director), Anjalique Lawrence (Assistant Director), Larry Crosland, Kush Malhotra, Bradley Becker, Lee McCracken, and Jayne Wilson.

Field Code Changed

Formatted: Heading 1

Related GAO Products

High-Risk Series: An Update, GAO-11-278. Washington, D.C.: February 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO-11-43. Washington, D.C.: November 30, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO-11-24. Washington, D.C.: October 6, 2010.

Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems. GAO-10-916. Washington, D.C.: September 15, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO-10-872T. Washington, D.C.: July 22, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving

Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development. GAO-10-466. Washington, D.C.: June 3, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO-10-513. Washington, D.C.: May 27, 2010.

Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements. GAO-10-202. Washington, D.C.: March 12, 2010.

Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. GAO-10-237. Washington, D.C.: March 12, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

(311067)