



Testimony
Before the Committee on Homeland
Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, June 16, 2010

CYBERSECURITY

Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues



G A O

Accountability * Integrity * Reliability

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



Highlights of [GAO-10-834T](#), a testimony before the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government. In recent testimony, the Director of National Intelligence highlighted that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the United States information infrastructure for intelligence collection, intellectual property theft, or disruption. In July 2009, press accounts reported attacks on Web sites operated by major government agencies. The ever-increasing dependence of federal agencies on information systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important that the federal government carry out a concerted effort to safeguard its systems and the information they contain.

GAO is providing a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make federal systems vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area.

[View GAO-10-834T or key components.](#)
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

CYBERSECURITY

Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats

What GAO Found

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and cyber attackers can easily preserve their anonymity. Further, the interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks. Consistent with this, reports of security incidents from federal agencies are on the rise, increasing by over 400 percent from fiscal year 2006 to fiscal year 2009.

Compounding the growing number and kinds of threats, GAO—along with agencies' internal assessments—has identified significant deficiencies in the security controls on federal information systems, which have resulted in pervasive vulnerabilities. These include weaknesses in the security of both financial and non-financial systems and information, including vulnerabilities in critical federal systems. These deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, and critical operations at risk of disruption.

Multiple opportunities exist to improve federal cybersecurity. To address identified deficiencies in agencies' security controls and shortfalls in their information security programs, GAO and agency inspectors general have made hundreds of recommendations over the past several years, many of which agencies are implementing. In addition, the White House, the Office of Management and Budget, and certain federal agencies have undertaken several governmentwide initiatives intended to enhance information security at federal agencies. While progress has been made on these initiatives, they all face challenges that require sustained attention, and GAO has made several recommendations for improving the implementation and effectiveness of these initiatives. Further, the Department of Homeland Security also needs to fulfill its key cybersecurity responsibilities, such as developing capabilities for ensuring the protection of cyber-based critical infrastructures and implementing lessons learned from a major cyber simulation exercise. Finally, a GAO-convened panel of experts has made several recommendations for improving the nation's cybersecurity strategy. Realizing these opportunities for improvement can help ensure that the federal government's systems, information, and critical cyber-based infrastructures are effectively protected.

Chairman Thompson and Members of the Committee:

Thank you for the opportunity to testify at today's hearing on cybersecurity regarding our recent work on challenges facing federal efforts to protect systems and critical infrastructure from cyber-based threats.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal systems and operations. In February 2010, the Director of National Intelligence testified that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the U.S. information infrastructure for intelligence collection, intellectual property theft, or disruption.¹ As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

In my testimony today, I will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make federal systems vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement in June 2010, we relied on our previous reports on federal information security. These reports 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

¹ Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, statement before the Senate Select Committee on Intelligence (Feb. 2, 2010).

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 have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions without these information assets. Information security is thus critically important. Conversely, ineffective information security controls can result in significant risks. Examples of such risks include the following:

- Resources, such as federal payments and collections, could be lost or stolen.
- Sensitive information, such as national security information, taxpayer data, Social Security records, medical records, and proprietary business information, could be inappropriately accessed and used for identity theft or espionage.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services could be disrupted.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Federal Systems and Infrastructures Face Increasing Cyber Threats

Threats to federal information systems and cyber-based critical infrastructures 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. Furthermore, as we have previously reported,² the techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can easily remain anonymous.

The connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. 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

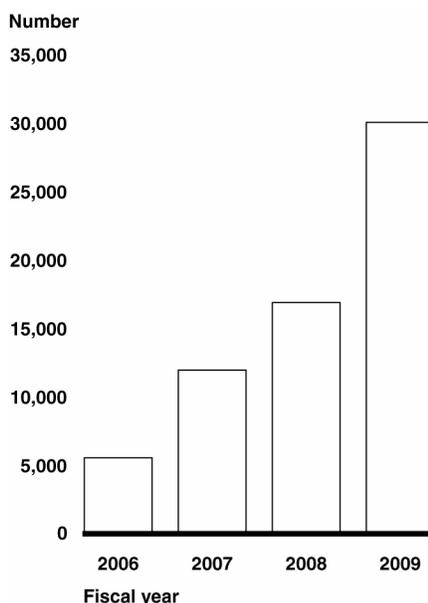
Consistent with the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about U.S. citizens has been lost, stolen, or improperly disclosed,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

² GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the Department of Homeland Security's (DHS) federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 4 years, from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009 (over a 400 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2009



Source: GAO analysis of US-CERT data.

The four most prevalent types of incidents and events reported to US-CERT during fiscal year 2009 were: (1) malicious code (software that infects an operating system or application), (2) improper usage (a violation of acceptable computing use policies), (3) unauthorized access (where an individual gains logical or physical access to a system without permission), and (4) investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

Vulnerabilities Pervade Federal Information Systems

The growing threats and increasing number of reported incidents highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. GAO has designated information security as a high-risk area in the federal government since 1997.

In their fiscal year 2009 performance and accountability reports, 21 of 24 major federal agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency.³

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example, we reported in September 2008⁴ that, although the Los Alamos National Laboratory—one of the nation’s weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas. Similarly, in October 2009⁵ we reported that the National Aeronautics and Space Administration (NASA)—the civilian agency that oversees

³ A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis.

⁴ GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

⁵ GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

U.S. aeronautical and space activities—had not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems supporting its mission directorates.

Opportunities Exist for Enhancing Federal Cybersecurity

Over the past several years, we and agency 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 certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies. However, these initiatives face challenges that require sustained attention:

- *Comprehensive National Cybersecurity Initiative (CNCI)*: In January 2008, President Bush initiated a series of 12 projects aimed primarily at improving the Department of Homeland Security's (DHS) and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.⁶ The initiative is intended to reduce

⁶ The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems. As we recently reported,⁷ the White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. However, the initiative faces challenges in achieving its objectives related to securing federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goals.

- *Federal Desktop Core Configuration (FDCC)*: For this initiative, OMB directed agencies that have workstations with Windows XP and/or Windows Vista operating systems to adopt security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs. We recently reported⁸ that while agencies have taken actions to implement FDCC requirements, none of the agencies has fully implemented all configuration settings on their applicable workstations. In our report we recommended that OMB, among other things, issue guidance on assessing the risks of agencies having deviations from the approved settings and monitoring compliance with FDCC.
- *Einstein*: This is a computer network intrusion detection system that analyzes network flow information from participating federal agencies and is intended to provide a high-level perspective from which to observe potential malicious activity in computer network traffic. We recently reported⁹ that as of September 2009, fewer than half of the 23 agencies reviewed had executed the required agreements with DHS, and Einstein 2 had been deployed to 6

⁷ GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Mar. 5, 2010).

⁸ GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements*, GAO-10-202 (Washington, D.C.: Mar. 12, 2010).

⁹ GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, D.C.: Mar. 12, 2010).

agencies. Agencies that participated in Einstein 1 cited improved identification of incidents and mitigation of attacks, but determining whether the initiative is meeting its objectives will likely remain difficult because DHS lacks performance measures that address how agencies respond to alerts.

- *Trusted Internet Connections (TIC) Initiative:* This is an effort designed to optimize individual agency network services through a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence. We recently reported¹⁰ that none of the 23 agencies we reviewed met all of the requirements of the TIC initiative, and most agencies experienced delays in their plans for reducing and consolidating connections. However, most agencies reported that they have made progress toward reducing and consolidating their external connections and implementing security capabilities.

DHS Needs to Fully Satisfy Its Cybersecurity Responsibilities

Federal law and policy¹¹ establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures¹²—a responsibility known as cyber critical infrastructure protection, or cyber CIP. We have reported since 2005 that DHS has yet to fully satisfy its key responsibilities for protecting these critical infrastructures. Our reports included recommendations that are essential for DHS to address in order to fully implement its

¹⁰ GAO-10-237.

¹¹ These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace*.

¹² 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. Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water.

responsibilities. We summarized these recommendations into key areas listed in table 1.

Table 1: Key Cybersecurity Areas Identified by GAO

- | |
|--|
| 1. Bolstering cyber analysis and warning capabilities |
| 2. Improving cybersecurity of infrastructure control systems |
| 3. Strengthening DHS's ability to help recover from Internet disruptions |
| 4. Reducing organizational inefficiencies |
| 5. Completing actions identified during cyber exercises |
| 6. Developing sector-specific plans that fully address all of the cyber-related criteria |
| 7. Securing internal information systems |

Source: GAO.

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department still has not fully implemented our recommendations, and thus further action needs to be taken to address these areas. For example, in July 2008, we reported¹³ that DHS's US-CERT did not fully address 15 key attributes of cyber analysis and warning capabilities related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. 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.

Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned

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

from these efforts.¹⁴ However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the department had identified 16 activities as ongoing and 7 as planned for the future.¹⁵ Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. Since that time, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

Improving the National Cybersecurity Strategy

Because the threats to federal information systems and critical infrastructure have persisted and grown, efforts have recently been undertaken by the executive branch to review the nation's cybersecurity strategy. In February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, creating a new national cybersecurity strategy, and developing a framework for cyber research and development.¹⁶ In response to one of these actions, the president appointed a cybersecurity coordinator in December 2009. We recently initiated a review to assess the progress made by the executive branch in implementing the report's recommendations.

¹⁴ GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

¹⁵ At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

¹⁶ The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

We also testified in March 2009 on needed improvements to the nation's cybersecurity strategy.¹⁷ In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 2.

Table 2: Key Strategy Improvements Identified by Cybersecurity Experts

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3. Establish a governance structure for strategy implementation.
4. Publicize and raise awareness about the seriousness of the cybersecurity problem.
5. Create an accountable, operational cybersecurity organization.
6. Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7. Bolster public-private partnerships through an improved value proposition and use of incentives.
8. Focus greater attention on addressing the global aspects of cyberspace.
9. Improve law enforcement efforts to address malicious activities in cyberspace.
10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11. Increase the cadre of cybersecurity professionals.
12. Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area.¹⁸ Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk of attack from our adversaries.

¹⁷ GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

¹⁸ We are currently conducting additional reviews related to these improvements.

In summary, the threats to federal information systems are evolving and growing, and federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with malicious intent have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. To help in meeting these threats, opportunities exist to improve information security throughout the federal government. The prompt and effective implementation of the hundreds of recommendations by us and by agency inspectors general to mitigate information security control deficiencies and fully implement agencywide security programs would strengthen the protection of federal information systems, as would efforts by DHS to develop better capabilities to meet its responsibilities, and the implementation of recommended improvements to the national cybersecurity strategy. Until agencies fully and effectively implement these recommendations, federal information and systems will remain vulnerable.

Mr. Chairman, this completes my prepared statement. I would be happy to answer any questions you or other Members of the Committee 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 John de Ferrari (Assistant Director), Michael Gilmore (Assistant Director), Anjalique Lawrence (Assistant Director), Marisol Cruz, Nick Marinos, Lee McCracken, and David Plocher.