

GAO

Testimony

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

For Release on Delivery
Expected 2:00 p.m. EDT
Thursday, June 25, 2009

CYBERSECURITY

**Continued Federal Efforts
Are Needed to Protect
Critical Systems and
Information**

Statement of Gregory C. Wilshusen,
Director, Information Security Issues



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-835T](#), a testimony before the Subcommittee on Technology and Innovation, Committee on Science and Technology, House of Representatives

Why GAO Did This Study

Federal laws and policy have assigned important roles and responsibilities to the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) for securing computer networks and systems. DHS is charged with coordinating the protection of computer-reliant critical infrastructure—much of which is owned by the private sector—and securing its own computer systems, while NIST is responsible for developing standards and guidelines for implementing security controls over information and information systems.

GAO was asked to describe cybersecurity efforts at DHS and NIST—including partnership activities with the private sector—and the use of cybersecurity performance metrics in the federal government. To do so, GAO relied on its reports on federal information security and federal efforts to fulfill national cybersecurity responsibilities.

What GAO Recommends

GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. In addition, GAO has made about 60 recommendations to strengthen security over information systems supporting DHS's programs for border security and its terrorist watch list. DHS has actions planned and underway to implement them.

View [GAO-09-835T](#) or [key components](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

CYBERSECURITY

Continued Federal Efforts Are Needed to Protect Critical Systems and Information

What GAO Found

Since 2005, GAO has reported that DHS has yet to comprehensively satisfy its key cybersecurity responsibilities, including those related to establishing effective partnerships with the private sector. Shortcomings exist in key areas that are essential for DHS to address in order to fully implement its cybersecurity responsibilities (see table). DHS has since developed and implemented certain capabilities, but still has not fully satisfied aspects of these responsibilities and needs to take further action to enhance the public/private partnerships needed to adequately protect cyber critical infrastructure. GAO has also previously reported on significant security weaknesses in systems supporting two of the department's programs, one that tracks foreign nationals entering and exiting the United States, and one for matching airline passenger information against terrorist watch-list records. DHS has corrected information security weaknesses for systems supporting the terrorist watch-list, but needs to take additional actions to mitigate vulnerabilities associated with systems tracking foreign nationals.

Key Cybersecurity Areas Reviewed 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.

NIST plays a key role in providing important information security standards and guidance. Pursuant to its responsibilities under the Federal Information Security Management Act (FISMA), NIST has developed standards specifying minimum security requirements for federal information and information systems; and provided corresponding guidance that details the controls necessary for securing those systems. It has also been working with both public and private sector entities to enhance information security requirements. The resulting guidance and tools provided by NIST serve as important resources for federal agencies that can be applied to information security programs.

As GAO recently testified in May, opportunities exist to improve the metrics used to assess agency information security programs. According to the performance metrics established by the Office of Management and Budget (OMB), agencies reported increased compliance in implementing key information security control activities. However, GAO and agency inspectors general continue to report significant weaknesses in controls. This dichotomy exists in part because the OMB-defined metrics generally do not measure how well controls are implemented. As a result, reported metrics may provide an incomplete picture of an agency's information security program.

Chairman Wu and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on computer-based (cyber) security activities at the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST). Cybersecurity is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. The need for a vigilant approach to cybersecurity has been demonstrated by the pervasive and sustained cyber attacks against the United States and others that continue to pose significant risks to computer systems and networks and the operations and critical infrastructures that they support.

In my testimony today, I will describe cybersecurity activities at DHS and NIST, including those activities related to establishing public/private partnerships with the owners of critical infrastructure. In addition, I will discuss the use of cybersecurity-related metrics in the federal government. In preparing for this testimony, we relied on our previous reports on federal information security and on DHS's efforts to fulfill its national cybersecurity responsibilities. We also relied on a draft report of our review of agencies' implementation of the Federal Information Security Management Act (FISMA).¹ These reports contain detailed overviews of the scope of our work and the methodology we used.

The work on which this testimony 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 provides 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.

¹FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). It permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. The act also assigns specific responsibilities to agency heads and chief information officers, NIST, and the Office of Management and Budget (OMB).

Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these cyber assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their systems and data. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets, as the following examples illustrate:

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as personally identifiable information, intellectual property, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.² The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical infrastructures. As government, private sector, and personal activities continue to move to networked operations, digital systems add ever more capabilities, wireless systems become more ubiquitous, and the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow.

² Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

DHS Is a Focal Point for National Cybersecurity Efforts

Federal law and policy³ establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures⁴—a practice known as cyber critical infrastructure protection, or cyber CIP. In this capacity, the department has multiple cybersecurity-related roles and responsibilities. In 2005, we identified, and reported on, 13 key cybersecurity responsibilities.⁵ They include, among others, (1) developing a comprehensive national plan for CIP, including cybersecurity; (2) developing partnerships and coordinating with other federal agencies, state and local governments, and the private sector; (3) developing and enhancing national cyber analysis and warning capabilities; (4) providing and coordinating incident response and recovery planning, including conducting incident response exercises; and (5) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems.⁶ Within DHS, the National Protection and Programs Directorate has primary responsibility for assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.

DHS is also responsible for securing its own computer networks, systems, and information. FISMA requires the department to develop and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency. Within DHS, the Chief Information

³These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace*.

⁴Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations 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.

⁵GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005) and *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

⁶Control systems are computer-based systems that perform vital functions in many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing.

Officer is responsible for ensuring departmental compliance with federal information security requirements.

NIST Is Responsible for Establishing Federal Standards and Guidance for Information Security

FISMA tasks NIST—a component within the Department of Commerce—with responsibility for developing standards and guidelines, including minimum requirements, for (1) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency and (2) providing adequate information security for all agency operations and assets, except for national security systems. The act specifically required NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST also is required to develop a definition of and guidelines for detection and handling of information security incidents as well as guidelines developed in conjunction with the Department of Defense and the National Security Agency for identifying an information system as a national security system. Within NIST, the Computer Security Division of the Information Technology Laboratory is responsible for developing information security related standards and guidelines.

FISMA also requires NIST to take other actions that include:

- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;
- developing and periodically revising performance indicators and measures for agency information security policies and practices;
- evaluating private sector information security policies and practices and commercially available information technologies, to assess potential application by agencies to strengthen information security; and
- assisting the private sector, in using and applying the results of its activities required by FISMA.

In addition, the Cyber Security Research and Development Act⁷ required NIST to develop checklists to minimize the security risks for each hardware or software system that is, or likely to become, widely used within the federal government.

Metrics Established to Evaluate Information Security Programs

FISMA also requires the Office of Management and Budget (OMB) to develop policies, principles, standards, and guidelines on information security and to report annually to Congress on agency compliance with the requirements of the act. OMB has provided instructions to federal agencies and their inspectors general for preparing annual FISMA reports. These instructions focus on metrics related to the performance of key control activities such as developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, testing contingency plans, and certifying and accrediting systems. FISMA reporting provides valuable information on the status and progress of agency efforts to implement effective security management programs.

Recent Efforts to Improve National Cybersecurity Strategy

Because the threats to federal information systems and critical infrastructure have persisted and grown, President Bush in January 2008 began to implement a series of initiatives—commonly referred to as the Comprehensive National Cybersecurity Initiative aimed primarily at improving DHS’s and other federal agencies’ efforts to protect against intrusion attempts and anticipate future threats.⁸ Since then, President Obama (in February 2009) directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States’ cyber security 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

⁷Cyber Security Research and Development Act, Pub. L. No.107-305, 116 Stat. 2367 (Nov. 27, 2002).

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

cyber research and development.⁹ In addition, we testified in March 2009¹⁰ that a panel of experts identified 12 key areas of the national cybersecurity strategy requiring improvement, such as developing a national strategy that clearly articulates strategic objectives, goals, and priorities; bolstering the public/private partnership; and placing a greater emphasis on cybersecurity research and development.

DHS Has Yet to Fully Satisfy Its Cybersecurity Responsibilities

We have reported since 2005 that DHS has yet to comprehensively satisfy its key responsibilities for protecting computer-reliant critical infrastructures. Our reports included about 90 recommendations that we summarized into key areas, including those listed in table 1, that are essential for DHS to address in order to fully implement its responsibilities. 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.

Table 1: Key Cybersecurity Areas Reviewed 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.

Bolstering Cyber Analysis and Warning Capabilities

In July 2008, we identified¹¹ that cyber analysis and warning capabilities included (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

⁹The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

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

¹¹GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, [GAO-08-588](#) (Washington, D.C.: July 31, 2008).

actionable threat and mitigation information, and (4) responding to the threat. These four capabilities are comprised of 15 key attributes, including establishing a baseline understanding of the nation's critical network assets and integrating analysis work into predictive analyses of broader implications or potential future attacks.

We concluded that while DHS's United States Computer Emergency Readiness Team (US-CERT) demonstrated aspects of each of the key attributes, it did not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtained information from numerous external information sources; however, it had not established a baseline of the nation's critical network assets and operations. In addition, while it investigated whether identified anomalies constituted actual cyber threats or attacks as part of its analysis, it did not integrate its work into predictive analyses of broader implications or potential future attacks, nor did it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provided warnings by developing and distributing a wide array of attack and other notifications; however, these notifications were not consistently actionable or timely—i.e., providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while the team responded to a limited number of affected entities in its efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, it did not possess the resources to handle multiple events across the nation.

We also concluded that without fully implementing the key attributes, US-CERT did not have the full complement of cyber analysis and warning capabilities essential to effectively perform its national mission. As a result, we made 10 recommendations to the department to address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS concurred and agreed to implement 9 of our 10 recommendations.

Improving Cybersecurity of Infrastructure Control Systems

In a September 2007 report and October 2007 testimony, we reported¹² that DHS was sponsoring multiple control systems security initiatives, including an effort to improve control systems cybersecurity using

¹²GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, [GAO-07-1036](#) (Washington, D.C.: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, [GAO-08-119T](#) (Washington, D.C.: Oct. 17, 2007).

Strengthening DHS's Ability to Help Recovery from Internet Disruption

vulnerability evaluation and response tools. However, DHS had not established a strategy to coordinate the various control systems activities across federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information. In response, DHS recently began developing a strategy and a process to share sensitive information.

We reported and later testified¹³ in 2006 that the department had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery in case of a major disruption. However, we determined that these efforts were not comprehensive or complete. As such, we recommended that DHS implement nine actions to improve the department's ability to facilitate public/private efforts to recover the Internet.

In October 2007, we testified¹⁴ that the department had made progress in implementing our recommendations; however, seven of the nine had not been completed. For example, it revised key plans in coordination with private industry infrastructure stakeholders, coordinated various Internet recovery-related activities, and addressed key challenges to Internet recovery planning. However, it has not, among other things, finalized recovery plans and defined the interdependencies among DHS's various working groups and initiatives. In other words, it has not completed an integrated private/public plan for Internet recovery. As a result, we concluded that the nation lacked direction from the department on how to respond in such a contingency. We also noted that these incomplete efforts indicated that DHS and the nation were not fully prepared to respond to a major Internet disruption. To date, an integrated public/private plan for Internet recovery does not exist.

¹³GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, [GAO-06-863T](#) (Washington, D.C.: July 28, 2006); and *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, [GAO-06-672](#) (Washington, D.C.: June 16, 2006).

¹⁴GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, [GAO-08-212T](#) (Washington, D.C.: Oct. 23, 2007).

Reducing Organizational Inefficiencies

In June 2008, we reported¹⁵ on the status of DHS's efforts to establish an integrated operations center that it agreed to adopt per recommendations from a DHS-commissioned expert task force. We determined that while DHS had taken the first step towards integrating two operations centers—the National Coordination Center Watch and US-CERT, it had yet to implement the remaining steps, complete a strategic plan, or develop specific tasks and milestones for completing the integration. We concluded that until the two centers were fully integrated, DHS was at risk of being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need. As a result, we recommended that the department complete its strategic plan and define tasks and milestones for completing remaining integration steps so that we are better prepared to provide an integrated response to disruptions to the communications infrastructure. DHS concurred with our first recommendation and stated that it would address the second recommendation as part of finalizing its strategic plan.

Completing Corrective Actions Identified During a Cyber Exercise

In September 2008, we reported¹⁶ on a major DHS-coordinated cyber attack exercise called Cyber Storm, which occurred in 2006 and included large-scale simulations of multiple concurrent attacks involving the federal government, states, foreign governments, and private industry. We determined that DHS had identified eight lessons learned from this exercise, such as the need to improve interagency coordination groups and the exercise program. We also concluded that while DHS had demonstrated progress in addressing the lessons learned, more needed to be done. Specifically, while the department completed 42 of the 66 activities identified to address the lessons learned, it identified 16 activities as ongoing and 7 as planned for the future.¹⁷ In addition, DHS provided no timetable for the completion dates of the ongoing activities. We noted that until DHS scheduled and completed its remaining activities, it was at risk of conducting subsequent exercises that repeated the lessons

¹⁵GAO, *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruption on Converged Voice and Data Networks*, [GAO-08-607](#) (Washington, D.C.: June 26, 2008).

¹⁶GAO, *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).

¹⁷At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

Developing Sector Specific
Plans that Fully Address All of
the Cyber-Related Criteria

learned during the first exercise. Consequently, we recommended that DHS schedule and complete the identified corrective activities so that its cyber exercises can help both public and private sector participants coordinate their responses to significant cyber incidents. DHS agreed with the recommendation. To date, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

In 2007, we reported and testified¹⁸ on the cybersecurity aspects of CIP plans for 17 critical infrastructure sectors, referred to as sector-specific plans. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors. DHS guidance requires each of the sector-specific agencies to develop plans to address how the sectors' stakeholders would implement the national plan and how they would improve the security of their assets, systems, networks, and functions.

We determined that none of the plans fully addressed the 30 key cybersecurity-related criteria described in DHS guidance. Further, while several sectors' plans fully addressed many of the criteria, others were less comprehensive. In addition to the variations in the extent to which the plans covered aspects of cybersecurity, there was also variance among the plans in the extent to which certain criteria were addressed. Consequently, we recommended¹⁹ that DHS request that the sector-specific agencies, fully address all cyber-related criteria by September 2008 so that stakeholders within the infrastructure sectors will effectively identify, prioritize, and protect the cyber aspects of their CIP efforts. We are currently reviewing the progress made in the sector specific plans.

We testified in March 2009²⁰ regarding the need to bolster public/private partnerships associated with cyber CIP. According to panel members, there are not adequate economic and other incentives (i.e. a value proposition) for greater investment and partnering with owners and operators of critical cyber assets and functions. Accordingly, panelists

¹⁸GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, [GAO-08-64T](#) (Washington D.C.: October 31, 2007) and *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, [GAO-08-113](#) (Washington D.C.: Oct. 31, 2007).

¹⁹[GAO-08-113](#).

²⁰[GAO-09-432T](#).

Securing Internal Information Systems

stated that the federal government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cybersecurity-related resources. We are also currently initiating a review of the status of the public/private partnerships in cyber CIP.

Besides weaknesses relating to external cybersecurity responsibilities, DHS had not secured its own information systems. In July 2007, we reported²¹ that DHS systems supporting the US-VISIT program²² were riddled with significant information security control weaknesses that place sensitive information—including personally identifiable information—at increased risk of unauthorized and possibly undetected disclosure and modification, misuse, and destruction, and place program operations at increased risk of disruption. Weaknesses existed in all control areas and computing device types reviewed. For example, DHS had not implemented controls to effectively prevent, limit, and detect access to computer networks, systems, and information. To illustrate, it had not (1) adequately identified and authenticated users in systems supporting US-VISIT, (2) sufficiently limited access to US-VISIT information and information systems, and (3) ensured that controls adequately protected external and internal network boundaries. In addition, it had not always ensured that responsibilities for systems development and system production had been sufficiently segregated, and had not consistently maintained secure configurations on the application servers and workstations at a key data center and ports of entry. As a result, intruders, as well as government and contractor employees, could potentially bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These acts could include tampering with data; browsing sensitive information; using computer resources for inappropriate purposes, such as launching attacks on other organizations; and disrupting or disabling computer-supported operations. According to the department, it has started remediation activities to

²¹GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, [GAO-07-870](#) (Washington, D.C.: July 13, 2007).

²²The US-VISIT program was established by DHS to record and track the entry and departure of foreign visitors who pass through U.S. ports of entry by air, land, or sea; to verify their identities; and to authenticate their travel documentation.

strengthen security over these systems and implement our recommendations.

In January 2009, we briefed congressional staff on security weaknesses associated with the development of systems supporting the Transportation Security Administration's (TSA) Secure Flight program.²³ Specifically, TSA had not taken sufficient steps to ensure that operational safeguards and substantial security measures were fully implemented to minimize the risk that the systems will be vulnerable to abuse and unauthorized access from hackers and other intruders. For example, TSA had not completed testing and evaluating key security controls, performed disaster recovery tests, or corrected high- and moderate-risk vulnerabilities. Accordingly, we recommended that TSA take steps to complete security testing, mitigate known vulnerabilities, and update key security documentation prior to initial operations. TSA subsequently undertook a number of actions to complete these activities. In May 2009, we concluded that TSA had generally met its requirements related to systems information security and satisfied our recommendations.²⁴

NIST Has Developed Important Federal Information Security Standards and Guidelines

NIST has taken steps to address its FISMA-mandated responsibilities by developing a suite of required security standards and guidelines as well as other publications that are intended to assist agencies in developing and implementing information security programs and effectively managing risks to agency operations and assets. In addition to developing specific standards and guidelines, NIST developed a set of activities to help agencies manage a risk-based approach for an effective information security program. These activities are known as the NIST Risk Management Framework. Several special publications support this framework and collectively provide guidance that agencies can apply to their information security programs for selecting the appropriate security controls for information systems—including the minimum controls necessary to protect individuals and the operations and assets of the organization.

²³This briefing contained information on our initial January 2009 assessment and recommendations. TSA, a component of DHS, developed an advanced passenger prescreening program known as Secure Flight that will allow TSA to match airline passenger information against terrorist watch-list records.

²⁴GAO, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, [GAO-09-292](#) (Washington, D.C.: May 13, 2009).

NIST has developed and issued the following documents to meet its FISMA mandated responsibilities:

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. This standard addresses NIST's requirement for developing standards for categorizing information and information systems. It requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The security categories are based on the harm or potential impact to an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.
- Special Publication 800-60 Volume I, revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. This guide is to assist federal government agencies with categorizing information and information systems. It is intended to help agencies consistently map security impact levels to types of (1) information (e.g., privacy, medical, proprietary, financial, investigation); and (2) information systems (e.g., mission critical, mission support, administrative). Furthermore, it is intended to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.
- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. This is the second of the mandatory security standards and specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. Specifically, this standard specifies minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies are required to meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53.
- Special Publication 800-61, revision 1, *Computer Security Incident Handling Guide*, March 2008. This publication is intended to assist organizations in establishing computer security incident response

capabilities and handling incidents efficiently and effectively. It provides guidelines for organizing a computer security incident response capability; handling incidents from initial preparation through post-incident lessons learned phase; and handling specific types of incidents, such as denial of service, malicious code, unauthorized access, and inappropriate usage.

- Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003. The purpose of this guide is to assist agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems.
- Special Publication 800-55, revision 1, *Performance Measurement Guide for Information Security*, July 2008. The purpose of this guide is to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs.
- Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. It also provides information on the selection of cost-effective security controls that can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.
- Special Publication 800-18, revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. This guide provides basic information on how to prepare a system security plan and is designed to be adaptable in a variety of organizational structures and used as a reference by those having assigned responsibility for activities related to security planning.

NIST is also in the process of developing, updating, and revising a number of special publications related to information security, including the following:

- Special Publication 800-37, revision 1, *Guide for Security Authorization of Federal Information Systems*, August 2008. This publication is intended to, among other things, support the development of a common security authorization process for federal information systems. According to NIST, the new security authorization process changes the traditional focus from the stove-pipe, organization-centric, static-based approaches and provides the capability to more effectively manage information system-related security risks in highly dynamic environments of complex and

sophisticated cyber threats, ever increasing system vulnerabilities, and rapidly changing missions. The process is designed to be tightly integrated into enterprise architectures and ongoing system development life cycle processes, promote the concept of near real-time risk management, and capitalize on current and previous investments in technology, including automated support tools.

- Special Publication 800-39, second public draft, *Managing Risk from Information Systems An Organizational Perspective*, April 2008. The purpose of this publication is to provide guidelines for managing risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation and use of information systems. According to NIST, the risk management concepts described in the publication are intentionally broad-based, with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST security standards and guidelines.
- Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, June 2009. This publication has been updated from the previous versions to include a standardized set of management, operational, and technical controls intended to provide a common specification language for information security for federal information systems processing, storing, and transmitting both national security and non national security information.
- Draft IR-7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*. This publication defines proposed measures for the severity of software security configuration issues and provides equations that can be used to combine the measures into severity scores for each configuration issue.

In addition, NIST has other ongoing and planned activities that are intended to enhance information security programs, processes, and controls. For example, it is supporting the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies. To support implementation of the credentialing program and aid security assessments, NIST is participating or will participate in the following initiatives:

- **Training** includes development of training courses, NIST publication quick start guides, and frequently asked questions to establish a common understanding of the standards and guidelines supporting the NIST Risk Management Framework.

-
- **Product and Services Assurance Assessment** includes defining criteria and guidelines for evaluating products and services used in the implementation of controls outlined in NIST SP 800-53.
 - **Support Tools** includes identifying or developing common protocols, programs, reference materials, checklists, and technical guides supporting implementation and assessment of SP 800-53-based security controls in information systems.
 - **Mapping initiative** includes identifying common relationships and the mappings of FISMA standards, guidelines, and requirements with International Organization for Standardization (ISO) standards for information security management, quality management, and laboratory testing and accreditation.

These planned efforts include implementing a program for validating security tools.

Other Collaborative Activities Undertaken by NIST

NIST collaborated with a broad constituency—federal and nonfederal—to develop documents to assist information security professionals. For example, NIST worked with the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems to develop a common process for authorizing federal information systems for operation. This resulted in a major revision to NIST Special Publication 800-37, currently issued as an initial public draft. NIST also collaborated with these organizations on Special Publication 800-53 and Special Publication 800-53A to provide guidelines for selecting and specifying security controls for federal government information systems and to help agencies develop plans and procedures for assessing the effectiveness of these controls. NIST also interacted with the DHS to incorporate guidance on safeguards and countermeasures for federal industrial control systems in Special Publication 800-53.

NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the ISO and International Electrotechnical Commission Information Security Management System standard. For example, the latest draft of Special Publication 800-53 introduces a three-part strategy for harmonizing the FISMA security standards and guidelines with international security standards including an updated mapping table for security controls.

NIST also undertook other information security activities, including

- developing Federal Desktop Core Configuration checklists and
- continuing a program of outreach and awareness through organizations such as the Federal Computer Security Program Managers' Forum and the Federal Information Systems Security Educators' Association.

Through NIST's efforts, agencies have access to additional tools and guidance that can be applied to their information security programs.

Opportunities for Improving Information Security Metrics

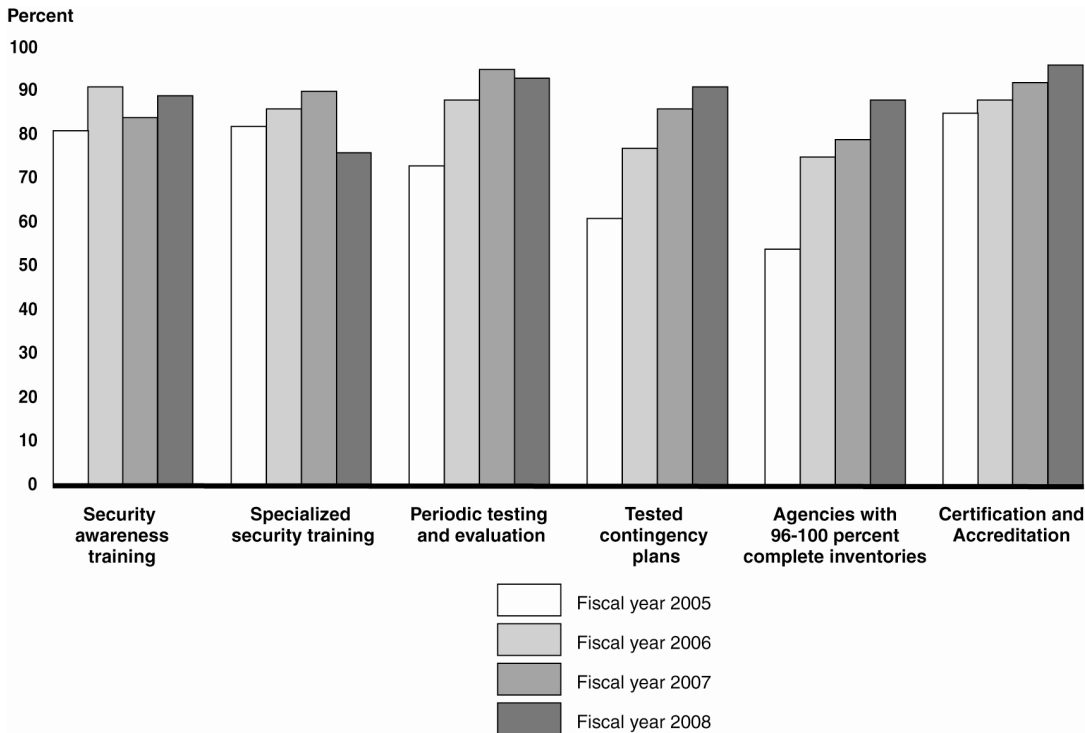
Despite federal agencies reporting increased compliance in implementing key information security control activities for fiscal year 2008, opportunities exist to improve the metrics used in annual reporting. The information security metrics developed by OMB focus on compliance with information security requirements and the implementation of key control activities. OMB requires federal agencies to report on key information security control activities as part of the FISMA-mandated annual report on federal information security. To facilitate the collection and reporting of information from federal agencies, OMB developed a suite of information security metrics, including the following:

- percentage of employees and contractors receiving security awareness training,
- percentage of employees with significant security responsibilities receiving specialized security training,
- percentage of systems tested and evaluated annually,
- percentage of systems with tested contingency plans,
- percentage of agencies with complete inventories of major systems, and
- percentage of systems certified and accredited.

In May 2009, we testified²⁵ that federal agencies generally reported increased compliance in implementing most of the key information security control activities for fiscal year 2008, as illustrated in figure 1.

²⁵ GAO, *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist*, [GAO-09-701T](#) (Washington, D.C.: May 19, 2009).

Figure 1: Selected Performance Metrics for Agency Systems



Source: GAO analysis of IG and agency data.

However, reviews at 24 major federal agencies²⁶ continue to highlight deficiencies in their implementation of information security policies and procedures. For example, in their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that their information system controls over their financial systems and information

²⁶The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

were either a material weakness or a significant deficiency.²⁷ In addition, 23 of the 24 agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. We also reported that agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply encryption to protect sensitive data on networks and portable devices; and (5) log, audit, and monitor security-relevant events. Furthermore, those agencies also had weaknesses in their agencywide information security programs.

An underlying reason for the apparent dichotomy of increased compliance with security requirements and continued deficiencies in security controls is that the metrics defined by OMB and used for annual information security reporting do not generally measure the effectiveness of the controls and processes that are key to implementing an agencywide security program. Results of our prior and ongoing work indicated that, for example, annual reporting did not always provide information on the quality or effectiveness of the processes agencies use to implement information security controls. Providing information on the effectiveness of controls and processes could further enhance the usefulness of the data for management and oversight of agency information security programs.

In summary, DHS has not fully satisfied aspects of its key cybersecurity responsibilities, one of which includes its efforts to protect our nation's cyber critical infrastructure and still needs to take further action to address the key areas identified in our recent reports, including enhancing partnerships with the private sector. In addition, although DHS has taken actions to remedy security weaknesses in its Secure Flight program, it still needs to address our remaining recommendations for strengthening

²⁷ A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. 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 misstatements on a timely basis.

controls for systems supporting the US-VISIT program. In taking these actions, DHS can improve its own information security as well as increase its credibility to external parties in providing leadership on cybersecurity. NIST has developed a significant number of standards and guidelines for information security and continues to assist organizations in implementing security controls over their systems and information. While NIST's role is to develop guidance, it remains the responsibility of federal agencies to effectively implement and sustain sufficient security over their systems. Developing and using metrics that measure how well agencies implement security controls can contribute to increased focus on the effective implementation of federal information security.

Chairman Wu, this concludes my statement. I would be happy to answer questions at the appropriate time.

Contact and Acknowledgements

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Other key contributors to this report include Michael Gilmore (Assistant Director), Charles Vrabel (Assistant Director), Bradley Becker, Larry Crosland, Lee McCracken, and Jayne Wilson.

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.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

