United States Government Accountability Office

GAO

Testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, July 19, 2005

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Addressing Cybersecurity

Statement of David A. Powner,
Director, Information Technology
Management Issues

G A O
Accountability * Integrity * Reliability

GAO-05-827T

July 2005

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Addressing Cybersecurity

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-05-827T, a Testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve cybersecurity of our nation's critical infrastructure.

www.gao.gov/cgi-bin/getrpt?GAO-05-827T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

As the focal point for CIP, the Department of Homeland Security (DHS) has many cybersecurity-related roles and responsibilities that GAO identified in law and policy (see table below for 13 key responsibilities). DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures.

While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity-related CIP responsibilities. These key challenges include achieving organizational stability, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, and achieving two-way information sharing with these stakeholders. In its strategic plan for cybersecurity, DHS identifies steps that can begin to address the challenges. However, until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. In recent years, GAO has made a series of recommendations to enhance the cybersecurity of critical infrastructures that if effectively implemented could greatly improve our nation's cybersecurity posture.

Table: DHS's Key Cybersecurity Responsibilities

• Develop a national plan for critical infrastructure protection, including cybersecurity. • Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. • Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities. • Develop and enhance national cyber analysis and warning capabilities. • Provide and coordinate incident response and recovery planning efforts.	• Identify and assess cyber threats and vulnerabilities. • Support efforts to reduce cyber threats and vulnerabilities. • Promote and support research and development efforts to strengthen cyberspace security. • Promote awareness and outreach. • Foster training and certification. • Enhance federal, state, and local government cybersecurity. • Strengthen international cyberspace security. • Integrate cybersecurity with national security.

Source: GAO analysis of law and policy.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing on challenges in protecting our nation's critical infrastructures from cybersecurity threats. Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support.

As requested, my testimony will focus on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection as established in law and policy, (2) the status of DHS's efforts to enhance the protection of the computer systems that support the nation's critical infrastructures and to strengthen information security—both inside and outside the federal government, (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities, and (4) recommendations we have made to improve cybersecurity of national critical infrastructures. In preparing for this testimony, we relied on our previous work on critical infrastructure protection and cybersecurity threats; primarily on a recent report on the challenges faced by DHS in fulfilling its cybersecurity responsibilities.[1] All of the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

As the focal point for critical infrastructure protection, DHS has many cybersecurity-related responsibilities that are called for in law and policy. These responsibilities include developing plans, building

[1]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434 (Washington, D.C.: May 26, 2005).

partnerships, and improving information sharing, as well as implementing activities related to the five priorities in the national cyberspace strategy: (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. To fulfill its cybersecurity role, in June 2003, the department established the National Cyber Security Division to serve as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts.

While DHS has initiated multiple efforts, it has not fully addressed any of the 13 key cybersecurity-related responsibilities that we identified in federal law and policy, and it has much work ahead in order to be able to fully address them. For example, DHS (1) has recently issued the *Interim National Infrastructure Protection Plan,* which includes cybersecurity elements; (2) operates the United States Computer Emergency Readiness Team to address the need for a national analysis and warning capability; and (3) has established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed national threat and vulnerability assessments or developed and exercised government and government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. Further, DHS continues to have difficulties in developing partnerships—as called for in federal policy—with other federal agencies, state and local governments, and the private sector.

DHS faces a number of challenges that have impeded its ability to fulfill its cyber-related critical infrastructure protection (CIP) responsibilities. Key challenges include achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal agencies, state and local governments and the private sector); achieving two-way information sharing with these stakeholders; and demonstrating the value it can provide. In

its strategic plan for cybersecurity, the department has identified steps that can begin to address these challenges. However, until it effectively confronts and resolves these underlying challenges, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our nation's critical infrastructures, and our nation will lack the strong cybersecurity focal point envisioned in federal law and policy.

Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures, focusing on the need to (1) develop a strategic analysis and warning capability for identifying potential cyberattacks, (2) protect infrastructure control systems, (3) enhance public/private information sharing, and (4) conduct important threat and vulnerability assessments and address other challenges to effective cybersecurity. Effectively implementing these recommendations could greatly improve our nation's cybersecurity posture.

Background

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. In recent years, the sophistication and effectiveness of cyberattacks have steadily advanced. These attacks often take advantage of flaws in software code, circumvent signature-based tools[2] that commonly identify and prevent known threats, and use social engineering techniques designed to trick the unsuspecting user into divulging sensitive information or propagating attacks. These attacks are becoming increasingly automated with the use of botnets—compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots)

[2] Signature-based tools compare files or packets to a list of "signatures"—patterns of specific files or packets that have been identified as threats.

have become a key automation tool used to speed the infection of vulnerable systems.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence-gathering, and acts of war. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

Recent attacks and threats have further underscored the need to bolster the cybersecurity of our government's and our nation's computer systems and, more importantly, of the critical operations and infrastructures they support. Recent examples of attacks include the following:

- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have adequately fortified their defenses against a potential catastrophic strike.
- In January 2005, a major university reported that a hacker had broken into a database containing 32,000 student and employee Social Security numbers, potentially compromising their identities and finances. In similar incidents during 2003 and 2004, it was reported that hackers had attacked the systems of other universities, exposing the personal information of over 1.8 million people.
- In June 2003, the U.S. government issued a warning concerning a virus that specifically targeted financial institutions. Experts said the BugBear.b virus was programmed to determine whether a victim had used an e-mail address for any of the roughly 1,300

financial institutions listed in the virus's code. If a match was found, the software attempted to collect and document user input by logging keystrokes and then provided this information to a hacker, who could use it in attempts to break into the banks' networks.

- In November 2002, a British computer administrator was indicted on charges that he accessed and damaged 98 computers in 14 states between March 2001 and March 2002, causing some $900,000 in damage. These networks belonged to the Department of Defense, the National Aeronautics and Space Administration, and private companies. The indictment alleges that the attacker was able to gain administrative privileges on military computers, copy password files, and delete critical system files. The attacks rendered the networks of the Earle Naval Weapons Station in New Jersey and the Military District of Washington inoperable.

In May 2005, we reported that federal agencies are facing a set of emerging cybersecurity threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms.[3] Examples of these threats include *spam* (unsolicited commercial e-mail), *phishing* (fraudulent messages used to obtain personal or sensitive data), and *spyware* (software that monitors user activity without the user's knowledge or consent). Spam consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; phishing can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government services; and spyware can capture and release sensitive data, make unauthorized changes, and decrease system performance.

[3] GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 13, 2005).

DHS's Responsibilities for Cybersecurity in Support of Critical Infrastructure Protection Are Many and Varied

Federal law and policies call for critical infrastructure protection (CIP) activities that are intended to enhance the cyber and physical security of both the public and private infrastructures that are essential to national security, national economic security, and national public health and safety.[4] Federal policy designates certain federal agencies as lead federal points of contact for the critical infrastructure sectors and assigns them responsibility for infrastructure protection activities in their assigned sectors and for coordination with other relevant federal agencies, state and local governments, and the private sector to carry out related responsibilities (see app. 1). In addition, federal policy establishes the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure information systems. To accomplish this mission, DHS is to work with other federal agencies, state and local governments, and the private sector.

Among the many CIP responsibilities established for DHS and identified in federal law and policy are 13 key cybersecurity-related responsibilities. These include general CIP responsibilities that have a cyber element (such as developing national plans, building partnerships, and improving information sharing) as well as responsibilities that relate to the five priorities established by the *National Strategy to Secure Cyberspace*. The five priorities are (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. Table 1 provides a description of each of these responsibilities.

[4]This law and these policies include the Homeland Security Act of 2002, Homeland Security Presidential Directive 7, and the *National Strategy to Secure Cyberspace*.

Table 1: Thirteen DHS Cybersecurity Responsibilities

General CIP responsibilities with a cyber element	Description
Develop a national plan for critical infrastructure protection that includes cybersecurity.	Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	Fostering and developing public/private partnerships with and among other federal agencies, state and local governments, the private sector, and others. DHS is to serve as the "focal point for the security of cyberspace."
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	Improving and enhancing information sharing with and among other federal agencies, state and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities.
Responsibilities related to the cyberspace strategy's five priorities	
Develop and enhance national cyber analysis and warning capabilities.	Providing cyber analysis and warnings, enhancing analytical capabilities, and developing a national indications and warnings architecture to identify precursors to attacks.
Provide and coordinate incident response and recovery planning efforts.	Providing crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cybersecurity continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
Identify and assess cyber threats and vulnerabilities.	Leading efforts by the public and private sector to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.
Support efforts to reduce cyber threats and vulnerabilities.	Leading and supporting efforts by the public and private sector to reduce threats and vulnerabilities. Threat reduction involves working with law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborating and coordinating with members of academia, industry, and government to optimize cybersecurity related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
Promote awareness and outreach.	Establishing a comprehensive national awareness program to promote efforts to strengthen cybersecurity throughout government and the private sector, including the home user.
Foster training and certification.	Improving cybersecurity-related education, training, and certification opportunities.
Enhance federal, state, and local government cybersecurity.	Partnering with federal, state, and local governments in efforts to strengthen the cybersecurity of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.
Strengthen international cyberspace security.	Working in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cybersecurity on a global basis.
Integrate cybersecurity with national security.	Coordinating and integrating applicable national preparedness goals with its National Infrastructure Protection Plan.

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace*.

In June 2003, DHS established the National Cyber Security Division (NCSD), under its Information Analysis and Infrastructure Protection Directorate, to serve as a national focal point for addressing cybersecurity issues and to coordinate implementation of the cybersecurity strategy. NCSD also serves as the government lead on a public/private partnership supporting the U.S. Computer Emergency Response Team (US-CERT) and as the lead for federal government incident response. NCSD is headed by the Office of the Director and includes a cybersecurity partnership program as well as four branches: US-CERT Operations, Law Enforcement and Intelligence, Outreach and Awareness, and Strategic Initiatives.

DHS Has Initiated Efforts That Begin to Address Its Responsibilities, but More Work Remains

DHS has initiated efforts that begin to address each of its 13 key responsibilities for cybersecurity; however, the extent of progress varies among these responsibilities, and more work remains to be done on each. For example, DHS (1) has recently issued an interim plan for infrastructure protection that includes cybersecurity plans, (2) is supporting a national cyber analysis and warning capability through its role in US-CERT, and (3) has established forums to build greater trust and to encourage information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed a national cyber threat assessment and sector vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy. The importance of such assessments is illustrated in our recent reports on vulnerabilities in infrastructure control systems and in wireless networks.[5] Further, the department has not yet developed and exercised government and government/industry contingency

[5]GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, (Washington, D.C.: Mar. 15, 2004) and *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*, GAO-05-383, (Washington, D.C.: May 17, 2005).

recovery plans for cybersecurity, including a plan for recovering key Internet functions. The department also continues to have difficulties in developing partnerships, as called for in federal policy, with other federal agencies, state and local governments, and the private sector. Without such partnerships, it is difficult to develop the trusted, two-way information sharing that is essential to improving homeland security.

Table 2 provides an overview of the steps that DHS has taken related to each of its 13 key responsibilities and identifies the steps that remain.

Table 2: Overview of Progress and Remaining Activities on DHS's 13 Cybersecurity-related Responsibilities

DHS Responsibility	DHS Progress	Status/What Remains
Develop a national plan for critical infrastructure protection that includes cybersecurity.	Issued Interim National Infrastructure Protection Plan that includes cybersecurity-related initiatives	The plan is not yet comprehensive and complete. DHS plans to add sector-specific cybersecurity details and milestones in subsequent versions.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	Undertook numerous initiatives to foster partnerships and enhance information sharing with other federal agencies, state and local governments, and the private sector about cyber attacks, threats, and vulnerabilities. Initiatives include the National Cyber Security Response System and Information Sharing and Analysis Center (ISAC) partnerships.	Information sharing has been limited. More work is needed to address barriers to effective partnerships and information sharing.
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.		
Develop and enhance national cyber analysis and warning capabilities.	Provides cyber analysis and warning capabilities through continuous operational support of the US-CERT; is working to enhance tools and communication mechanisms for providing analysis and warning of potential cyber incidents.	Efforts are not complete. DHS has not yet developed the indications and warning architecture required by HSPD-7, and important analytical tools are not yet mature.
Provide and coordinate incident response and recovery planning efforts.	Improved ability to coordinate a response to cyber attacks with federal, state, and local governments and private-sector entities through the communications capabilities developed for US-CERT, continued expansion of backup communication capabilities, and establishment of collaboration mechanisms.	Plans and exercises for recovering from attacks are not yet complete and comprehensive. DHS does not yet have plans for testing federal continuity plans, recovering key Internet functions, or providing technical assistance to both private-sector and other government entities as they develop their own emergency recovery plans
Identify and assess cyber threats and vulnerabilities.	Participated in national efforts to identify and assess cyber threats and has begun taking steps to facilitate sector-specific vulnerability assessments	Assessments are not yet complete.DHS has not yet completed the comprehensive cyber threat and vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy.

Support efforts to reduce cyber threats and vulnerabilities.	Initiated efforts to reduce threats by enhancing collaboration with the law enforcement community and to reduce vulnerabilities by shoring up guidance on software and system security	Efforts are not complete. Vulnerability reduction efforts are limited until the cyber-related vulnerability assessments (discussed in the previous section) are completed.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborated with the Executive Office of the President and with other federal departments and agencies to develop a national research and development plan for CIP, including cybersecurity.	A comprehensive plan is not yet in place, and the milestones for key activities have not yet been established. The stakeholders expect to issue a plan with a roadmap, investment plan, and milestones next year.
Promote awareness and outreach.	Made progress in increasing cybersecurity awareness by implementing numerous awareness and outreach initiatives, including the National Cyber Alert System, the National Cyber Security Awareness Month program, and the US CERT public Web site.	The effectiveness of awareness and outreach activities is unclear. Many CIP stakeholders are still uncertain of DHS's cybersecurity roles.
Foster training and certification.	Initiated multiple efforts to improve the education of future cybersecurity analysts, including cosponsoring the National Centers of Academic Excellence in Information Assurance program and fostering the scholarship for service program.	Efforts are not yet complete. Much work remains to be done to develop certification standards.
Enhance federal, state, and local government cybersecurity.	Supports multiple interagency groups' efforts to improve government cybersecurity, including the Chief Information Security Officers forum, the National Cyber Response Coordination Group, and the Government Forum of Incident Response and Security Teams.	Efforts are not yet complete. State and local government stakeholders have expressed concerns about the scope of these efforts .
Strengthen international cyberspace security.	Works in conjunction with other foreign governments to promote a global culture of security. Initiatives include participation in the G-8 High Tech Crime working group and the International Watch and Warning Framework/Multilateral Conference.	More remains to be done. DHS plans to create and pursue an international strategy to secure cyberspace and to promote collaboration, coordination, and information sharing with international communities.
Integrate cybersecurity with national security.	Formed the National Cyber Response Coordinating Group—a forum of national security, law enforcement, defense, intelligence, and other government agencies—that coordinates intragovernmental and public/private preparedness and response to and recovery from national-level cyber incidents and physical attacks that have significant cyber consequences.	Important testing remains to be done. Early tests of this coordination showed the need to improve communication protocols; additional testing is warranted.

Source: GAO analysis of DHS information.

DHS Continues to Face Challenges in Establishing Itself as a National Focal Point for Cyberspace Security

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. Key challenges include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders (other federal, state, and local governments and the private sector), achieving two-way information sharing with these stakeholders, and providing and demonstrating the value DHS can provide.

Organizational stability: Over the last year, multiple senior DHS cybersecurity officials—including the NCSD Director, the Deputy Director responsible for Outreach and Awareness, and the Director of the US-CERT Control Systems Security Center, the Under Secretary for the Information Analysis and Infrastructure Protection Directorate and the Assistant Secretary responsible for the Information Protection Office—have left the department. Infrastructure sector officials stated that the lack of stable leadership has diminished NCSD's ability to maintain trusted relationships with its infrastructure partners and has hindered its ability to adequately plan and execute activities. According to one private-sector representative, the importance of organizational stability in fostering strong partnerships cannot be over emphasized.

Organizational authority: NCSD does not have the organizational authority it needs to effectively serve as a national focal point for cybersecurity. Accordingly, its officials lack the authority to represent and commit DHS to efforts with the private sector. Infrastructure and cybersecurity officials, including the chairman of the sector coordinators and representatives of the cybersecurity industry, have expressed concern that the cybersecurity division's relatively low position within the DHS organization hinders its ability to accomplish cybersecurity-related goals. NCSD's lack of authority has led to some missteps, including DHS's cancellation of an important cyber event without explanation and its taking almost a year to issue formal responses to private sector recommendations

that resulted from selected National Cyber Security Summit task forces—even though responses were drafted within months.

A congressional subcommittee also expressed concern that DHS's cybersecurity office lacks the authority to effectively fulfill its role. In 2004 and again in 2005, the subcommittee proposed legislation to elevate the head of the cybersecurity office to an assistant secretary position. Among other benefits, the subcommittee reported that such a change could

- provide more focus and authority for DHS's cybersecurity mission,
- allow higher level input into national policy decisions, and
- provide a single visible point of contact within the federal government for improving interactions with the private sector.

Hiring and contracting: Ineffective DHS management processes have impeded the department's ability to hire employees and maintain contracts. We recently reported that since DHS's inception, its leadership has provided a foundation for maintaining critical operations while it undergoes transformation.[6] However, in managing its transformation, we noted that the department still needed to overcome a number of significant challenges, including addressing systemic problems in human capital and acquisition systems. Federal and nonfederal officials expressed concerns about its hiring and contracting processes. For example, an NCSD official reported that the division has had difficulty in hiring personnel to fill vacant positions. These officials stated that once they found qualified candidates, some candidates decided not to apply and another one withdrew his acceptance because he felt that DHS's hiring process had taken too long. In addition, a cybersecurity division official stated that there had been times when DHS did not renew NCSD contracts in a timely manner, requiring that key contractors work without pay until approvals could be completed and payments could be made. In other cases, NCSD was denied services from a vendor because the department had repeatedly

[6]GAO, *High-Risk Series: An Update,* GAO-05-207, (Washington, D.C.: January, 2005).

failed to pay this vendor for its services. External stakeholders, including an ISAC representative, also noted that NCSD is hampered by how long it takes DHS to award a contract.

Awareness of DHS roles and capabilities: Many infrastructure stakeholders are not yet aware of DHS's cybersecurity roles and capabilities. Department of Energy critical infrastructure officials stated that the roles and responsibilities of DHS and the sector-specific agencies need to be better clarified in order to improve coordination. In addition, during a regional cyber exercise, private-sector and state and local government officials reported that the mission of NCSD and the capabilities that DHS could provide during a serious cyber-threat were not clear to them. NCSD's manager of cyber analysis and warning operations acknowledged that the organization has not done an adequate job reaching out to the private sector regarding the department's role and capabilities.

Effective partnerships: NCSD is responsible for leveraging the assets of key stakeholders, including other federal, state, and local governments and the private sector, in order to facilitate effective protection of cyber assets. The ability to develop partnerships greatly enhances the agency's ability to identify, assess, and reduce cyber threats and vulnerabilities, establish strategic analytical capabilities, provide incident response, enhance government cybersecurity, and improve international efforts. According to one infrastructure sector representative, effective partnerships require building relationships with mutually developed goals; shared benefits and responsibilities; and tangible, measurable results. However, this individual reported that DHS has not typically adopted these principles in pursuing partnerships with the private sector, which dramatically diminishes cybersecurity gains that government and industry could otherwise achieve. For example, it has often informed the infrastructure sectors about government initiatives or sought input after most key decisions have been made. Also, the department has not demonstrated that it recognizes the value of leveraging existing private sector mechanisms, such as information-sharing entities and processes that are already in place and working. In addition, the instability of NCSD's leadership positions to date has led to problems in developing partnerships. Representatives from two ISACs reported that turnover at the

cybersecurity division has hindered partnership efforts. Additionally, IT sector representatives stated that NCSD needs continuity of leadership, regular communications, and trusted policies and procedures in order to build the partnerships that will allow the private sector to share information.

Information sharing: We recently identified information sharing in support of homeland security as a high-risk area, and we noted that establishing an effective two-way exchange of information to help detect, prevent, and mitigate potential terrorist attacks requires an extraordinary level of cooperation and perseverance among federal, state, and local governments and the private sector.[7] However, such effective communications are not yet in place in support of our nation's cybersecurity. Representatives from critical infrastructure sectors stated that entities within their respective sectors still do not openly share cybersecurity information with DHS. As we have reported in the past, much of the concern is that the potential release of sensitive information could increase the threat to an entity. In addition, sector representatives stated that when information is shared, it is not clear whether the information will be shared with other entities—such as other federal entities, state and local entities, law enforcement, or various regulators—and how it will be used or protected from disclosure. Representatives from the banking and finance sector stated that the protection provided by the Critical Infrastructure Information Act and the subsequently established Protected Critical Infrastructure Information Program is not clear and has not overcome the trust barrier. Sector representatives have expressed concerns that DHS is not effectively communicating information to them. According to one infrastructure representative, DHS has not matched private sector efforts to share valuable information with a corresponding level of trusted information sharing. An official from the water sector noted that when representatives called DHS to inquire about a potential terrorist threat, they were told that DHS could not share any information and that they should "watch the news."

[7]GAO-05-207.

Providing value: According to sector representatives, even when organizations within their sectors have shared information with NCSD, the entities do not consistently receive useful information in return. They noted that without a clear benefit, they are unlikely to pursue further information sharing with DHS. Federal officials also noted problems in identifying the value that DHS provides. According to Department of Energy officials, the department does not always provide analysis or reports based on the information that agencies provide. Federal and nonfederal officials also stated that most of US-CERT's alerts have not been useful because they lack essential details or are based on already available information. Further, Treasury officials stated that US-CERT needed to provide relevant and timely feedback regarding the incidents that are reported to it.

Clearly, these challenges are not mutually exclusive. That is, addressing challenges in organizational stability and authority will help NCSD build the credibility it needs in order to establish effective partnerships and achieve two-way information sharing. Similarly, effective partnerships and ongoing information sharing with its stakeholders will allow DHS to better demonstrate the value it can add.

DHS has identified steps in its strategic plan for cybersecurity that can begin to address these challenges. Specifically, it has established goals and plans for improving human capital management that should help stabilize the organization. Further, the department has developed plans for communicating with stakeholders that are intended to increase awareness of its roles and capabilities and to encourage information sharing. Also, it has established plans for developing effective partnerships and improving analytical and watch and warning capabilities that could help build partnerships and begin to demonstrate added value. However, until it begins to address these underlying challenges, DHS cannot achieve significant results in coordinating cybersecurity activities, and our nation will lack the effective focal point it needs to better ensure the security of cyberspace for public and private critical infrastructure systems.

Implementation of GAO Recommendations Should Enhance Cybersecurity of Critical Infrastructures

Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures, focusing on the need to (1) develop a strategic analysis and warning capability for identifying potential cyberattacks, (2) protect infrastructure control systems, (3) enhance public/private information sharing, and (4) conduct important threat and vulnerability assessments and address other challenges to effective cybersecurity. These recommendations are summarized below.

Strategic Analysis and Warnings: In 2001, we reported on the analysis and warnings efforts within DHS's predecessor, the National Infrastructure Protection Center, and identified several challenges that were impeding the development of an effective strategic analysis and warning capability.[8] We reported that a generally accepted methodology for analyzing strategic cyber-based threats did not exist. Specifically, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. We also reported that the Center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies.

We therefore recommended that the responsible executive-branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data. However, officials have taken little action to establish this capability, and therefore our recommendations remain open today.

[8]GAO, C*ritical Infrastructure Protection: Significant Challenges in Developing National Capabilities,* GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

Control Systems: In March 2004, we reported that several factors—including the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems—contributed to an escalation of the risk of cyber-attacks against control systems.[9] We recommended that DHS develop and implement a strategy for coordinating with the private sector and with other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with our recommendation and, in December 2004, issued a high-level national strategy for control systems security. This strategy includes, among other things, goals to create a capability to respond to attacks on control systems and to mitigate vulnerabilities, bridge industry and government efforts, and develop control systems security awareness. However, the strategy does not yet include underlying details and milestones for completing activities.

Information Sharing: In July 2004, we recommended actions to improve the effectiveness of DHS's information-sharing efforts.[10] We recommended that officials within the Information Analysis and Infrastructure Protection Directorate (1) proceed with and establish milestones for developing an information-sharing plan and (2) develop appropriate DHS policies and procedures for interacting with ISACs, sector coordinators (groups or individuals designated to represent their respective infrastructure sectors' CIP activities), and sector-specific agencies and for coordination and information sharing within the Information Analysis and Infrastructure Protection Directorate and other DHS components. These recommendations remain open today. Moreover, we recently designated establishing appropriate and effective information-sharing mechanisms to improve homeland security as a new high-risk area.[11] We reported that the ability to share security-related information can unify the efforts of federal, state, and local

[9] GAO-04-354.

[10] GAO, C*ritical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004).

[11] GAO-05-207.

government agencies and the private sector in preventing or minimizing terrorist attacks.

Threat and Vulnerability Assessments and Other Challenges: Most recently, in May 2005, we reported that while DHS has made progress in planning and coordinating efforts to enhance cybersecurity, much more work remains to be done to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments and recovery plans. Further, we reported that DHS faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private/public assets and information in order to clearly demonstrate the value it can provide. We made recommendations to strengthen the department's ability to implement key cybersecurity responsibilities by prioritizing and completing critical activities and resolving underlying challenges.

We recently met with DHS's acting director for cybersecurity who told us that DHS agreed with our findings and has initiated plans to address our recommendations. He acknowledged that DHS has not adequately leveraged their public and private stakeholders in a prioritized manner and it plans to begin its prioritized approach by focusing stakeholders on information sharing, preparedness, and recovery. He also added that the next iteration of the *National Infrastructure Protection Plan* will focus on Internet recovery, control systems, and software assurance.

In summary, as our nation has become increasingly dependent on timely, reliable information, it has also become increasingly vulnerable to attacks on the information infrastructure that supports the nation's critical infrastructures (including the energy, banking and finance, transportation, telecommunications, and drinking water infrastructures). Federal law and policy acknowledge this by establishing DHS as the focal point for coordinating cybersecurity plans and initiatives with other federal agencies, state and local

governments, and private industry. DHS has made progress in planning and coordinating efforts to enhance cybersecurity, but much more work remains to be done for the department to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments and recovery plans.

As DHS strives to fulfill its mission, it faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private and public assets and information in order to clearly demonstrate the value it can provide. Until it overcomes the many challenges it faces and completes critical activities, DHS cannot effectively function as the cybersecurity focal point intended by law and national policy. As such, there is increased risk that large portions of our national infrastructure are either unaware of key areas of cybersecurity risks or unprepared to effectively address cyber emergencies. Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures. These include (1) developing a strategic analysis and warning capability for identifying potential cyberattacks, (2) protecting infrastructure control systems, (3) enhancing public/private information sharing, and (4) conducting important threat and vulnerability assessments and address other challenges to effective cybersecurity. Effectively implementing these recommendations could greatly improve our nation's cybersecurity posture.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-9286 or by e-mail at pownerd@gao.gov. Other key contributors to this report include Joanne Fiorino, Michael Gilmore, Barbarol James, Colleen Phillips, and Nik Rapelje.

Appendix I: Infrastructure Sectors and Lead Agencies Identified by Federal Policies on Critical Infrastructure Protection

Sector	Description	Lead agency
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	Department of Homeland Security
Dams	Comprises approximately 80,000 dam facilities, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Drinking water and water treatment systems	Sanitizes the water supply through about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security

Sector	Description	Lead agency
National monuments and icons	Includes key assets that are symbolically equated with traditional American values and institutions or U.S. political and economic power.	Department of the Interior
Nuclear reactors, materials, and waste	Includes 104 commercial nuclear reactors; research and test nuclear reactors; nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.	Department of Homeland Security working with the Nuclear Regulatory Agency and Department of Energy
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation systems	Enables movement of people and of assets that are vital to our economy, mobility, and security via aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security in collaboration with the Department of Transportation

Source: GAO analysis based on the President's National Strategy documents and HSPD-7.