United States Government Accountability Office

GAO

Testimony

Before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

For Release on Delivery
Expected at 3 p.m. EDT
Wednesday, September 13, 2006

CRITICAL INFRASTRUCTURE PROTECTION

DHS Leadership Needed to Enhance Cybersecurity

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

G A O
Accountability * Integrity * Reliability

GAO-06-1087T

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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.

September 13, 2006

GAO
Accountability • Integrity • Reliability
Highlights

Highlights of GAO-06-1087T, a testimony before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

CRITICAL INFRASTRUCTURE PROTECTION

DHS Leadership Needed To Enhance Cybersecurity

Why GAO Did This Study

Increasing computer interconnectivity has revolutionized the way that 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 establish 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 recent reports on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection and for recovering the Internet in case of a major disruption (2) challenges facing DHS in addressing its cybersecurity responsibilities, including leadership challenges, and (3) recommendations to improve the cybersecurity of national critical infrastructures, including the Internet.

www.gao.gov/cgi-bin/getrpt?GAO-06-1087T.

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

In 2005 and 2006, GAO reported that DHS had initiated efforts to address its responsibilities for enhancing the cybersecurity of critical infrastructures, but that more remained to be done. Specifically, in 2005, GAO reported that DHS had initiated efforts to fulfill 13 key cybersecurity responsibilities, but it had not fully addressed any of them. For example, DHS established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities, but had not developed national threat and vulnerability assessments for cybersecurity. Since that time, DHS has made progress on its 13 key responsibilities—including the release of its *National Infrastructure Protection Plan*—but none have been completely addressed. Moreover, in 2006, GAO reported that DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not complete or comprehensive. For example, DHS established working groups to facilitate coordination among government and industry infrastructure officials and fostered exercises in which government and private industry could practice responding to cyber events, but many of its efforts lacked timeframes for completion and the relationships among its various initiatives were not evident.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity responsibilities, including establishing effective partnerships with stakeholders, demonstrating the value it can provide to private sector infrastructure owners, and reaching consensus on DHS's role in Internet recovery and on when the department should get involved in responding to an Internet disruption. DHS faces a particular challenge in attaining the organizational stability and leadership it needs to gain the trust of other stakeholders in the cybersecurity world—including other government agencies as well as the private sector. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department. In July 2005, DHS undertook a reorganization which established the position of the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, over a year later, this position remains vacant.

To strengthen DHS's ability to implement its cybersecurity responsibilities and to resolve underlying challenges, GAO has made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. These recommendations provide a high-level road map for DHS to use to help improve our nation's cybersecurity posture. Until they are addressed, DHS will have difficulty achieving results as the federal cybersecurity focal point.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing on the need for leadership 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.

Federal regulation establishes the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis and warning, information sharing, vulnerability reduction, and recovery efforts for public and private critical infrastructure information systems.[1] Additionally, federal policy recognizes the need to be prepared for the possibility of debilitating Internet disruptions and—because the vast majority of the Internet's infrastructure is owned and operated by the private sector—tasks DHS with developing an integrated public/private plan for Internet recovery.[2]

As requested, our testimony will summarize our recent work on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection and, more specifically, its responsibilities for recovering the Internet in case of a major disruption, (2) challenges facing DHS in addressing its cybersecurity responsibilities, including leadership challenges, and (3) recommendations to improve the cybersecurity of national critical infrastructures, including the Internet. In preparing for this testimony, we relied on our previous reports on the challenges faced by DHS in fulfilling its cybersecurity responsibilities and in

[1]Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003).

[2]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

facilitating the recovery of the Internet in case of a major disruption.[3] These reports contain detailed overviews of the scope and methodology we used. 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. In 2005 and 2006, we reported that DHS had initiated efforts to address these responsibilities, but that more remained to be done.[4] Specifically, in 2005, we reported that DHS had initiated efforts to fulfill 13 key cybersecurity responsibilities, but it had not fully addressed any of them. For example, DHS established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities, but had not developed national threat and vulnerability assessments for cybersecurity. Since that time, DHS has made progress on its responsibilities—including the release of its National Infrastructure Protection Plan—but none has been completely addressed. Moreover, in 2006, we reported that DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but that these efforts were not complete or comprehensive. For example, DHS had established working groups to facilitate coordination among government and industry infrastructure officials and fostered exercises in which government and private industry could practice responding to cyber events, but many of its efforts lacked

[3]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434 (Washington, D.C.: May 26, 2005); *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*,GAO-05-827T (Washington, D.C.: July 19, 2005); *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006); *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-863T (Washington, D.C.: July 28, 2006).

[4]GAO-05-434 and GAO-06-672.

timeframes for completion and the relationships among its various initiatives are not evident.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity responsibilities, including establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, demonstrating the value it can provide to private sector infrastructure owners, and reaching consensus on DHS's role in Internet recovery and on when the department should get involved in responding to an Internet disruption. DHS faces a particular challenge in attaining the organizational stability and leadership it needs to gain the trust of other stakeholders in the cybersecurity world—including other government agencies as well as the private sector. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department. In July 2005, DHS undertook a reorganization which established the position of the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, over a year later, this position remains vacant. While DHS stated that the lack of a permanent assistant secretary has not hampered its efforts related to protecting critical infrastructures, several private-sector representatives stated that DHS's lack of leadership in this area has limited its progress.

To strengthen DHS's ability to implement its cybersecurity responsibilities and to resolve underlying challenges, GAO has made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct important threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. Together, the recommendations provide a high-level road map for DHS to use in working to improve our nation's cybersecurity posture. Until it addresses these recommendations, DHS will have difficulty achieving results in its role as the federal focal point for the cybersecurity of critical infrastructures—including the Internet.

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[5] 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.

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

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

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 were 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 January 2003, the Slammer worm infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet by exploiting a known vulnerability for which a patch had been available for 6 months.[6] Slammer caused network outages, canceled airline flights, and automated teller machine failures. In addition, the Nuclear Regulatory Commission confirmed that the Slammer worm had infected a private computer network at a nuclear power plant, disabling a safety monitoring system for nearly 5 hours and causing the plant's process computer to fail. The worm reportedly also affected communication on the control networks of at least five utilities by propagating so quickly that control system traffic was

[6]GAO-06-672.

blocked. Cost estimates on the impact of the work range from $1.05 billion to $1.25 billion.

In May 2005, we reported that federal agencies were facing a set of emerging cybersecurity threats as a result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms.[7] 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. These attacks are also 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) have become a key automation tool that is used to speed the infection of vulnerable systems.

Federal law and regulation call for critical infrastructure protection 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.[8] Federal regulation also establishes 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. Federal policy further recognizes the need to prepare for debilitating Internet disruptions and—because the vast majority of the Internet infrastructure is

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

[8]The Homeland Security Act of 2002 and the Homeland Security Presidential Directive 7.

owned and operated by the private sector—tasks the DHS with developing an integrated public/private plan for Internet recovery.[9]

Prior Reports Identified DHS's Efforts to Fulfill Cybersecurity Responsibilities

As the focal point for critical infrastructure protection, the Department of Homeland Security (DHS) has many cybersecurity-related roles and responsibilities that are called for in law and policy. These responsibilities include developing plans, building partnerships, and improving information sharing, as well as implementing activities related to the five priorities in the *National Strategy to Secure Cyberspace*. These 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. See table 1 for a list of DHS's 13 key cybersecurity responsibilities. These responsibilities are described in more detail in appendix I. To fulfill its cybersecurity role, in June 2003, DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures.

[9]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

Table 1: DHS's Key Cybersecurity Responsibilities

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

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

In our 2005 report and testimony, we noted that while DHS initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 responsibilities, and much work remained to fulfill them.[10] 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 had not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity. Since that report was issued, DHS has made progress on its responsibilities, but none have been completely addressed. For example, in June 2006, the agency released the National Infrastructure Protection Plan; however, supplemental sector-specific plans have not yet been finalized. Further, DHS reported that it has expanded the use of a situational awareness tool that supports cyber analysis and warning from one to seven federal

[10]GAO-05-434 and GAO-05-827T.

agencies. However, this does not yet comprise a national analysis and warning capability.

In our 2006 report and testimony, we focused particularly on one of DHS's key cybersecurity responsibilities—facilitating Internet recovery.[11] We reported that DHS had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but that these efforts were not comprehensive or complete. For example, DHS had developed high-level plans for infrastructure protection and incident response; however, the components of these plans that address the Internet infrastructure were not complete. Further, several representatives of private-sector firms supporting the Internet infrastructure expressed concerns about the plans, noting that the plans would be difficult to execute in times of crisis. The department had also started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including establishing working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress to date on these initiatives had been limited, and other initiatives lacked time frames for completion. Also, the relationships among these initiatives were not evident. As a result, we reported that the government was not yet adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption. A private-sector organization subsequently reported that our nation was unprepared to reconstitute the Internet after a massive disruption, noting that there were significant gaps in government response plans and that the responsibilities of the multiple organizations that would plan a role in recovery were unclear.[12]

[11] GAO-06-672 and GAO-06-863T.

[12] *Business Roundtable, Essential Steps to Strengthen America's Cyber Terrorism Preparedness* (Washington, D.C.: June 2006).

DHS Faces Many Challenges; Organizational Stability and Leadership Are Keys to Success

DHS faces numerous challenges in fulfilling its cybersecurity-related CIP responsibilities. Key challenges in fulfilling DHS's broad responsibilities include increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with these stakeholders, and demonstrating the value it can provide to private sector infrastructure owners. Key challenges to establishing a plan for recovering from Internet disruptions include addressing innate characteristics of the Internet that make planning for and responding to disruptions difficult, achieving consensus on DHS's role[13] and on when the department should get involved in responding to a disruption, addressing legal issues affecting DHS's ability to provide assistance to restore Internet service, and overcoming reluctance of many in the private sector to share information on Internet disruptions with DHS. Further, the department faces a particular challenge in attaining the organizational stability and leadership it needs to gain the trust of other stakeholders in the cybersecurity world—including other government agencies as well as the private sector.

In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department.[14] These officials included the NCSD Director, the Deputy Director responsible for Outreach and Awareness, 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.

[13]While some private sector officials we spoke to stated that the government did not have a direct recovery role, others identified a variety of potential roles including providing information on specific threats, providing security and disaster relief during a crisis, funding backup communication infrastructures, driving improved Internet security through requirements for the government's own procurements, and providing logistical assistance, such as fuel, power, and security to Internet infrastructure operators during a crisis.

[14]GAO-05-434.

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.

In July 2005, DHS underwent a reorganization which elevated responsibility for cybersecurity to an assistant secretary position. NCSD and the National Communication System were placed in the Preparedness Directorate under a new position, called the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, over a year later, this position remains vacant. While DHS stated that the lack of a permanent assistant secretary has not hampered its efforts related to protecting critical infrastructure, several private-sector representatives stated that DHS's lack of leadership in this area has limited progress. Specifically, these representatives stated that filling key leadership positions would enhance DHS's visibility to the Internet industry and would potentially improve its reputation.

Implementation of GAO's Recommendations Should Enhance DHS's Ability to Fulfill Cybersecurity Responsibilities and Address Challenges

To strengthen DHS's ability to implement its cybersecurity responsibilities and to resolve underlying challenges, GAO has made about 25 recommendations over the last several years. These recommendations focus on the need to (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption. These recommendations are summarized below and key recommendations that have not yet been fully implemented are listed in appendix 2. Together, the recommendations provide a high-level roadmap for DHS to use to improve our nation's cybersecurity posture. Until it

addresses these recommendations, DHS will have difficulty achieving results in its role as a federal focal point for cybersecurity of critical infrastructures.

Threat and Vulnerability Assessments: In May 2005, we reported that while DHS had made progress in planning and coordinating efforts to enhance cybersecurity, much more work remained to be done for the department to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments.[15] Specifically, we noted that DHS had participated in national efforts to identify and assess cyber threats and had begun to take steps to facilitate sector-specific vulnerability assessments, but that it had not completed a national cyber threat assessment, sector-specific vulnerability assessments, or the identification of cross-sector interdependencies that are called for in the cyberspace strategy. We made recommendations to strengthen the department's ability to implement key cybersecurity responsibilities by prioritizing and completing critical activities and resolving underlying challenges. DHS concurred with our recommendation to engage stakeholders in prioritizing its key cybersecurity responsibilities, including performing a national cyber threat assessment and facilitating sector cyber vulnerability assessments. However, these efforts are not yet complete.

Strategic Analysis and Warnings: In 2001, we reported on the analysis and warnings efforts within DHS's predecessor, the National Infrastructure Protection Center, and we identified several challenges that were impeding the development of an effective strategic analysis and warning capability.[16] 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.

[15]GAO-05-434.

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

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.

More recently, in 2005, we reported that DHS had established various initiatives to enhance its analytical capabilities, including intelligence-sharing through the US CERT and situational awareness tools through the US CERT Einstein program at selected federal agencies. However, we noted that DHS was still facing the same challenges in developing strategic analysis and warning capabilities and that our original recommendations had not been fully implemented.

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—had contributed to an escalation of the risk of cyber-attacks against control systems.[17] 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. In 2007, we plan to evaluate federal efforts to enhance the protection of critical control systems.

Information Sharing: Over the years, we have issued a series of reports, summarized below, on efforts to improve information sharing in support of critical infrastructure protection. Further,

[17]GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354 (Washington, D.C.: Mar. 15, 2004).

because of the importance of this topic, in January 2005, we designated establishing appropriate and effective information-sharing mechanisms to improve homeland security as a new high-risk area in our report on federal programs and operations at risk.[18] We reported that the ability to share security-related information can unify the efforts of federal, state, and local government agencies and the private sector in preventing or minimizing terrorist attacks.

In July 2004, we recommended actions to improve the effectiveness of DHS's information-sharing efforts.[19] 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. DHS stated that the report generally provided an accurate analysis and planned actions to address these recommendations. However, as of today, the recommendations have not yet been implemented.

More recently, in March 2006, we reported that more than 4 years after September 11, the nation still lacked governmentwide policies and processes to help agencies integrate a myriad of ongoing efforts to improve the sharing of terrorism-related information that is critical to protecting our homeland.[20] Responsibility for creating these policies and processes now lies with the Director of National Intelligence—and should include a cybersecurity focus. We made several recommendations to the Director of National Intelligence to strengthen information sharing efforts.

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

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

[20]GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: March 17, 2006).

Most recently, in April 2006, we reported on DHS's efforts to implement the Critical Infrastructure Information Act of 2002, which was enacted to encourage nonfederal entities to voluntarily share critical infrastructure information and established protections for it.[21] DHS has initiated several actions, including issuing interim operating procedures[22] and creating a program office to administer the critical infrastructure protection program called for by the Critical Infrastructure Information Act. The program office has also begun to accept and safeguard critical infrastructure information submitted voluntarily by infrastructure owners and is sharing it with other DHS entities and, on a limited basis, with other government entities. For example, as of January 2006, the program office had received about 290 submissions of critical infrastructure information from various sectors. However, DHS faces challenges that impede the private sector's willingness to share sensitive information, including defining specific government needs for critical infrastructure information, determining how the information will be used, assuring the private sector that the information will be protected and who will be authorized to have access to the information, and demonstrating to critical infrastructure owners the benefits of sharing the information. We recommended that DHS better define its own and other federal agencies' critical infrastructure information needs and explain how it and the other agencies will use the information they receive from the private sector. We also recommended that DHS establish a specific deadline for issuing its final operating procedures. DHS concurred with our findings and recommendations and has made progress in selected areas. Specifically, on September 1, 2006, DHS released its final operating procedures.[23]

[21]GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383 (Washington, D.C.: April 17, 2006).

[22]On February 20, 2004, DHS issued *Procedures for Handling Critical Infrastructure Information: Interim Rule* (69 FR 8074) that, among other things, included mechanisms specified in law, established authorities regarding the sharing of information, and stated that DHS would consider issuing supplemental regulations.

[23]Department of *Homeland Security, Procedures* for Handling Critical Infrastructure Information; Final Rule (71 FR 52262) (Sept. 1, 2006).

Recovery Planning: In May 2005, we reported that while DHS had made progress in planning and coordinating efforts to enhance cybersecurity, much more work remained to be done to fulfill its responsibilities—including facilitating government and government/industry cybersecurity recovery plans.[24] More recently, in June 2006, we reported that DHS had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but that these efforts were not complete or comprehensive.[25] Further, we reported that DHS faced key challenges in establishing a plan for recovering from Internet disruptions, including obtaining consensus on its role and on when the department should get involved in responding to a disruption, overcoming the reluctance of many in the private sector to share information on Internet disruptions, addressing leadership uncertainties within the department. We made recommendations to strengthen the department's ability to help recover from Internet disruptions. DHS concurred with our recommendations and identified plans to begin addressing them.

We also reported that the federal laws and regulations that address critical infrastructure protection, disaster recovery, and the telecommunications infrastructure provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, key legislation on critical infrastructure protection does not address roles and responsibilities in the event of an Internet disruption. Other laws and regulations governing disaster response and emergency communications have never been used for Internet recovery. We suggested that Congress consider clarifying the legal framework guiding Internet recovery.

In summary, while DHS has initiatives underway to fulfill its many cybersecurity responsibilities, major tasks remain to be done. These include assessing and reducing cyber threats and vulnerabilities and

[24]GAO-05-434.

[25]GAO-06-672.

coordinating incident response and recovery planning efforts. In fulfilling its cybersecurity responsibilities, DHS has many challenges to overcome, several of which will be difficult without effective leadership. Effective leadership is essential in order to fulfill key government responsibilities and to partner and build credibility with the private sector. Addressing this leadership void starts with DHS naming its Assistant Secretary of Cyber Security and Telecommunications. Once that position is filled, our recommendations in the areas of threat and vulnerability analysis, analysis and warning, control systems protection, information sharing, and recovery planning can help prioritize efforts to secure our nation's public and private infrastructures.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions at this time.

If you have any questions on matters discussed in this testimony, please contact us at (202) 512-9286 or by e-mail at pownerd@gao.gov. Other key contributors to this report include Colleen Phillips (Assistant Director), Vijay D'Souza, Michael Gilmore, Barbarol James, and Teresa Neven.

Appendix I: Thirteen DHS Cybersecurity Responsibilities

Critical infrastructure protection 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.*

Appendix II: Key Recommendations To Improve Cybersecurity of Critical Infrastructures

Functional Area	Recommendations That Have Not Yet Been Fully Implemented
Threat and vulnerability assessments	Perform a national cyber threat assessment.
	Facilitate sector cyber vulnerability assessments—to include identification of cross-sector interdependencies.
Strategic analysis and warning	Establish a capability for strategic analysis of computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data.
	Develop a comprehensive governmentwide data-collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources
	Develop a comprehensive written plan for establishing analysis and warning capabilities that integrates existing planning elements and includes milestones and performance measures; approaches (or strategies) and the various resources needed to achieve the goals and objectives; a description of the relationship between the long-term goals and objectives and the annual performance goals; and a description of how program evaluations could be used to establish or revise strategic goals, along with a schedule for future program evaluations.
Infrastructure control systems protection	Develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems.
Public/private information sharing	To ensure effective implementation of the Intelligence Reform Act, assess progress toward the milestones set in the Interim Implementation Plan; identify any barriers to achieving these milestones,such as insufficient resources and determine ways to resolve them; and recommend to the oversight committees with jurisdiction any necessary changes to the organizational structure or approach to creating the Information Sharing Environment.[26]
	Consistent with other infrastructure planning efforts such as the NIPP, define and communicate to the private sector what critical infrastructure information DHS and federal entities need to fulfill their critical infrastructure responsibilities and how federal, state, and local entities are expected to use the information submitted under the program.
	Determine whether creating mechanisms, such as providing originator control and direct submissions to federal agencies other than DHS, would increase submissions of critical infrastructure information.
	Expand efforts to use incentives to encourage more users of critical infrastructure information, such as mechanisms for state-to-state sharing.
	Proceed with and establish milestones for the development of an information-sharing plan that includes (1) a clear description of the roles and responsibilities of DHS, the ISACs, the sector coordinators, and the sector-specific agencies and (2) actions designed to address information-sharing challenges. Efforts to develop this plan should include soliciting feedback from the ISACs, sector coordinators, and sector-specific agencies to help ensure that challenges identified by the ISACs and the ISAC Council are appropriately considered in the final plan.
	Considering the roles, responsibilities, and actions established in the information-sharing plan, develop appropriate DHS policies and procedures for interacting with the Information Sharing and Analysis Centers (ISACs), sector coordinators, and sector-specific agencies and for coordination and information sharing within the IAIP Directorate (such as the National Cyber Security Division and Infrastructure Coordination Division) and other DHS components that may interact with the ISACs, including TSA.

[26]We made this recommendation to the Office of the Director of National Intelligence.

Functional Area	Recommendations That Have Not Yet Been Fully Implemented
Recovery planning	Establish contingency plans for cybersecurity, including recovery plans for key internet functions.
	Establish dates for revising the *National Response Plan* and finalizing the *National Infrastructure Protection Plan* (to include components related to Internet recovery).
	Draft public/private plans for Internet recovery and obtain input from key Internet infrastructure companies.
	Review the organizational structures and roles of DHS's National Communication System (NCS) and National Cyber Security Division (NCSD) in light of the convergence of voice and data communications.
	Identify the relationships and interdependencies among the various Internet recovery-related activities currently underway in NCS and NCSD.
	Establish timelines and priorities for key efforts identified by the Internet Disruption Working Group.
	Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.
	Work with private-sector stakeholders representing the Internet infrastructure to address challenges to effective Internet recovery by (1) further defining needed government functions, (2) defining a trigger for government involvement in responding to a disruption, and (3) documenting assumptions and developing approaches to deal with key challenges that are not within the government's control.
Crosscutting topics	Engage appropriate stakeholders to prioritize key cybersecurity responsibilities so that the most important activities are addressed first.
	Prioritize a list of activities for addressing underlying challenges that are impeding execution of DHS responsibilities
	Identify performance measures and milestones for fulfilling prioritized responsibilities and activities to address underlying challenges, and track progress against these measures and milestones

Source: GAO-06-383, GAO-06-385, GAO-06-672, GAO-05-434, GAO-04-780, GAO-04-354, and GAO-01-323.