United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, March 20, 2007

CRITICAL INFRASTRUCTURE

Challenges Remain in Protecting Key Sectors

Statement of

Eileen R. Larence, Director
Homeland Security and Justice Issues

David A. Powner, Director
Information Technology Management Issues

GAO-07-626T

March 20, 2007

CRITICAL INFRASTRUCTURE:

Challenges Remain in Protecting Key Sectors

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-626T, a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

Why GAO Did This Study

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures—both physical and cyber—have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy including formation of government and private sector councils as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures, in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP). This testimony is based primarily on GAO's October 2006 sector council report and a body of work on cyber critical infrastructure protection. Specifically, it addresses (1) the extent to which these councils have been established, (2) key facilitating factors and challenges affecting the formation of the council, (3) key facilitating factors and challenges encountered in developing sector plans, and (4) the status of DHS's efforts to fulfill key cybersecurity responsibilities.

GAO has made previous recommendations, particularly in the area of cybersecurity that have not been fully implemented. Continued monitoring will determine whether further recommendations are warranted.

www.gao.gov/cgi-bin/getrpt?GAO-07-626T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

To better coordinate infrastructure protection efforts as called for in the NIPP, all 17 critical infrastructure sectors have established their respective government councils, and nearly all sectors have initiated their voluntary private sector councils. But council progress has varied due to their characteristics and level of maturity. For example, the public health and healthcare sector is quite diverse and collaboration has been difficult as a result; on the other hand, the nuclear sector is quite homogenous and has a long history of collaboration. As a result, council activities have ranged from getting organized to refining infrastructure protection strategies. Ten sectors, such as banking and finance, had formed councils prior to development of the NIPP and had collaborated on plans for economic reasons, while others had formed councils more recently. As a result, the more mature councils could focus on strategic issues, such as recovering after disasters, while the newer councils were focusing on getting organized.

Council members reported mixed views on what factors facilitated or challenged their actions. For example, long-standing working relationships with regulatory agencies and within sectors were frequently cited as the most helpful factor. Challenges most frequently cited included the lack of an effective relationship with DHS as well as private sector hesitancy to share information on vulnerabilities with the government or within the sector for fear the information would be released and open to competitors. GAO's past work has shown that a lack of trust in DHS and fear that sensitive information would be released are recurring barriers to the private sector's sharing information with the federal government, and GAO has made recommendations to help address these barriers. DHS has generally concurred with these recommendations and is in the process of implementing them.

All the sectors met the December 2006 deadline to submit their sector-specific plans to DHS, although the level of collaboration between the sector and government councils on the plans, which the NIPP recognizes as critical to establishing relationships between the government and private sectors, varied by sector. Issuing the NIPP and completing sector plans are only first steps to ensure critical infrastructure is protected. Moving forward to implement sector plans and make progress will require continued commitment and oversight.

While DHS has initiatives under way to fulfill its many cybersecurity responsibilities, major tasks remain to be done. These include assessing and reducing cyber threats and vulnerabilities and coordinating incident response and recovery planning efforts. Effective leadership by the Assistant Secretary for Cyber Security and Telecommunications is essential to DHS fulfilling its key responsibilities, addressing the challenges, and implementing recommendations.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on infrastructure protection issues. The nation's critical infrastructures and key resources—including those cyber and physical assets essential to national security, national economic security, and national public health and safety—have been and continue to be vulnerable to a wide variety of threats. In 2005, Hurricane Katrina devastated the Gulf Coast, damaging critical infrastructure such as oil platforms, pipelines, and refineries; water mains; electric power lines; and cellular phone towers. The chaos resulting from this infrastructure damage disrupted the functioning of government and business alike and produced cascading effects far beyond the physical location of the storm. In 2004, authorities discovered a plan to target financial institutions in New York, and in 2005 suicide bombings struck London's public transportation system, disrupting the city's transportation and mobile telecommunications infrastructure. Because the private sector owns approximately 85 percent of the nation's critical infrastructure—such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities—it is vital that the public and private sectors form effective partnerships to successfully protect these assets.

A key player in these partnerships is the Department of Homeland Security (DHS). The Homeland Security Act of 2002 created DHS and gave it wide-ranging responsibilities for leading and coordinating the overall national critical infrastructure protection effort.[1] The act required DHS to develop a comprehensive national plan for securing the nation's critical infrastructures and recommend measures to protect key resources. Homeland Security Presidential Directive 7 (HSPD-7) further defined critical infrastructure protection responsibilities for DHS and those federal agencies given responsibility for particular industry sectors, such as transportation, energy, and telecommunications, known as sector-specific agencies. DHS is to establish uniform policies, approaches, guidelines, and methodologies to help ensure that critical infrastructure within and across the 17 infrastructure sectors is protected,[2] and is to use a risk management

[1]Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[2]These critical infrastructure and key resource sectors include agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, materials, and waste; dams;

approach to coordinate protection efforts. This includes using risk assessments to set priorities for protective measures by the department; sector-specific agencies; tribal, state, and local government agencies and authorities with critical assets and resources in their jurisdiction, owners and operators of these assets; and other entities.

HSPD-7 required DHS to develop a comprehensive and integrated plan by December 2004 that outlines national protection goals, objectives, milestones, and key initiatives necessary to fulfilling these responsibilities. In response, DHS developed the National Infrastructure Protection Plan (NIPP). Issued in June 2006, the NIPP is a base plan that is to serve as a road map for how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. In particular, the NIPP required the individual sector-specific agencies, working with relevant government and private sector representatives, to submit plans to DHS by the end of December 2006 that would establish the means by which the sectors will identify their critical assets, assess risks of terrorist attacks or other hazards on them, assess and prioritize those which have national significance, and develop protective measures for the sector. DHS is to use these individual plans to evaluate whether any gaps exist in the protection of critical infrastructures on a national level and, if so, to work with the sectors to address the gaps.

The NIPP describes a partnership model as the primary means of coordinating government and private sector efforts to protect critical infrastructure. For each sector, the model requires formation of government coordinating councils (government councils)—composed of federal, state, local, or tribal agencies with purview over critical assets—and encourages voluntary formation of sector coordinating councils (sector councils)—composed of owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations. Councils are to be representative, are to collaborate in

defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and health care; telecommunications; and transportation systems. Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, and national public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence. For purposes of this report, we will use the term "critical infrastructure" to also include key resources.

planning and implementing efforts to protect critical infrastructure, and are envisioned to focus on policy issues.

My testimony today highlights four key areas from our previously issued work: (1) the extent to which sectors have established councils, (2) the key facilitating factors and challenges that critical infrastructure protection stakeholders encountered in establishing their respective councils, (3) the key facilitating factors and challenges sectors encountered in developing their sector-specific plans, and (4) the status of DHS's efforts to fulfill key cybersecurity responsibilities and challenges. My comments today are based on GAO's October 2006 report addressing the progress made in coordinating government and private sector efforts to establish councils and develop sector-specific plans and on a body of GAO work related to cyber critical infrastructure protection that has been designated as a GAO high-risk area since 2003.[3] GAO's October 2006 report was based on work conducted at the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security,[4] Interior, and Treasury; the Environmental Protection Agency; as well as with private sector representatives of 14 councils.[5] We conducted our work in accordance with generally accepted government auditing standards.

In Summary

To help implement the NIPP and develop their own plans for protecting critical assets and key resources, each of the infrastructure sectors has established government councils, and voluntary private sector councils have been formed for all sectors except transportation systems. The characteristics and levels of maturity of these councils vary significantly across the sectors, which in turn has affected the progress sectors have

[3]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007); *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*, GAO-06-1087T (Washington, D.C.: Sept. 13, 2006); *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C: May 26, 2005); and *Internet Infrastructure: DHS Faces Challenges in Developing A Joint Public/Private Recovery Plan*, GAO-06-672 (June 16, 2006).

[4]DHS is the sector-specific agency for 10 sectors: information technology; telecommunications; transportation systems; chemical; emergency services; commercial nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities.

[5]The government facilities sector and the national monuments and icons sector do not have sector councils because they have no private sector components. As of March 2007, the transportation systems sector had yet to form a private sector council.

made in organizing and in developing their plans. For example, the public health and health care sector is quite diverse and collaboration has been difficult as a result; on the other hand, the nuclear sector is quite homogenous and has a long history of collaboration. As a result, council activities have ranged from just getting organized to refining their infrastructure protection strategies. To develop effective protection plans, it is important that council membership represent these unique and varied interests, and we found this generally to be true for most of the councils. The age and maturity of the councils also varied. Ten sectors had formed councils prior to the development of the NIPP model because they were already collaborating on protective measures, while the remaining sectors had formed councils more recently. The more mature councils, including banking and finance and telecommunications, were able to focus on strategic activities, such as developing plans on how to resume operations as soon as possible after a disaster. In contrast, the newer councils—including public health and healthcare and commercial facilities—were still focusing on identifying key stakeholders and members, developing charters, and getting organized. As of March 2007, the transportation systems sector had yet to form a sector council, but a DHS Infrastructure Protection official said each transportation mode—such as rail, aviation, and maritime—has established a sector council. According to DHS officials, once the modes are organized, the transportation systems council will be formed.

Representatives of the councils most frequently cited prior long-standing working relationships and effective information sharing within their sector as well as access to contractor resources through DHS as key in establishment of a number of the councils. Conversely, the lack of an effective relationship with DHS, private sector hesitancy to provide sensitive information on infrastructure vulnerabilities to the government or within the sector, and the lack of prior relationships with federal agencies or within the sector were the most frequently cited challenges to developing other councils. In terms of facilitating factors, sectors that had been regulated by federal agencies for years, such as the banking and finance sector, reported developing long-standing and trusted working relationships both with the federal agencies and within the sectors, which facilitated council development. These sectors also recognized the need to share information in order to collaborate on protection efforts. Another key facilitating factor was having access to resources and technical assistance from DHS contractors, filling resource and skill gaps some sectors had in establishing and operating their councils. In terms of challenges, some government and sector councils cited high turnover of some DHS staff and the staff's lack of understanding about infrastructure

operations as hindering council formation. While DHS officials reported that staff turnover should not affect the formation of sector councils because guidance is available to help councils, the officials said that this turnover could hinder the establishment of trusted working relationships. Representatives from various sectors also noted, as has our past work, that some in the private sector are reluctant to share sensitive infrastructure information with the federal government for fear the information might be publicly disclosed or make them subject to litigation for failure to disclose their vulnerabilities.

In August 2006, we found that each of the 17 sector-specific agencies was in the process of preparing a sector-specific plan to comply with the NIPP, but the sectors were at varying stages of completion. For example, the chemical and nuclear sectors said their plans were nearing completion, while the commercial facilities sector said its plan was still in outline form. Some in the private sector said collaboration between the sector council and the government council on the plans had yet to take place. Despite these differences, according to DHS Infrastructure Protection officials, all the sectors submitted their plans to DHS by the December 2006 deadline, and DHS and other stakeholders are in the process of reviewing them. Like the NIPP, these plans are only a first step; they are to lay out how the sector will identify its most critical assets and resources and what methodologies each will use to assess risks, but are not required to address how the sector is actually assessing risk and protecting its most critical assets. Council members cited as a key facilitating factor the fact that some sectors had prior plans that they could update to satisfy NIPP requirements. For example, the energy sector had developed a protection plan in anticipation of the Year 2000 (Y2K) computer threat, and that process was beneficial in developing its sector-specific plan for the NIPP. Two other frequently cited factors that helped with developing plans, as well as developing the councils themselves, were when sectors had pre-existing relationships with federal agencies or within the sector and access to contractor support through DHS. The most frequently cited challenges included the late issuance of a final NIPP that outlined stable requirements for the plans as well as the changing nature of DHS guidance on how to develop the plans. DHS periodically added new requirements on the risk assessment processes and on managing and coordinating sector responsibilities, some in response to industry comments. For example, DHS incorporated changes in the final NIPP in response to comments that it should better recognize the need to focus on both protecting against and recovering from a disaster. But, several council members said it was frustrating to have to update their protection plans multiple times in response to changes from the interim, draft, and the final NIPP. Finally,

several cited the heterogeneous characteristics of some sectors, such as the widely different industries that make up the agriculture and food sector, as making collaboration and consensus on their plans a challenge.

The protection of critical cyber assets and resources is particularly important because sectors depend on cyber infrastructure to operate. As a result, it is important that all sectors factor cyber infrastructure needs as part of their protection plans. As the focal point for critical infrastructure protection, DHS has many cybersecurity-related responsibilities that are called for in law and policy. While DHS has initiatives under way to fulfill its many cybersecurity responsibilities, major tasks remain to be done. These include assessing and reducing cyber threats and vulnerabilities and coordinating incident response and recovery planning efforts. 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 which are necessary to set priorities for protection investments. Since that time, DHS has made progress on its responsibilities—including the release of its NIPP—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. In addition, we reported that DHS faced a particular challenge in attaining the organizational stability and leadership it needed to gain the trust of other cybersecurity stakeholders —including other government agencies as well as the private sector. In July 2005, DHS undertook a reorganization that established the position of the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department and in September 2006, DHS announced that it had filled this position. Effective leadership by the Assistant Secretary is essential to DHS fulfilling its key responsibilities and addressing the challenges and recommendations. Overall, DHS has made progress with some critical infrastructure challenges, but we maintain that it must still address outstanding recommendations—such as better defining its critical infrastructure information needs and better explaining how this information will be used—and address cyber infrastructure vulnerabilities to be an effective federal focal point for critical infrastructure.

Background

Critical Infrastructure Protection Policy Has Emphasized Government and Private Sector Coordination

The protection of the nation's critical infrastructure against natural and man-made catastrophic events has been a concern of the federal government for over a decade. For example, in May 1998, Presidential Decision Directive 63 (PDD-63) established critical infrastructure protection as a national goal and presented a strategy for cooperative efforts by the government and the private sector to protect it.

In December 2003, HSPD-7 was issued, defining responsibilities for DHS and federal agencies responsible for addressing specific critical infrastructure sectors. These agencies are to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. DHS is to, among other things, coordinate national critical infrastructure protection efforts, establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors; and provide for the sharing of information essential to critical infrastructure protection. According to the NIPP, DHS is also to develop and implement comprehensive risk management programs and methodologies, develop cross-sector and cross-jurisdictional protection guidance, recommend risk management and performance criteria and metrics within and across sectors, and establish structures to enhance the close cooperation between the private sector and government at all levels.

In addition, DHS is 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 owned and operated by the private sector—tasks DHS with developing an integrated public/private plan for Internet recovery.[6]

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

Sector-Specific Agencies Are to Coordinate Protection Efforts and Develop Plans

HSPD-7 designated sector-specific agencies for each of the critical infrastructure sectors, responsible for coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector, and facilitating the sharing of information about threats, vulnerabilities, incidents, potential protective measures, and best practices. Agencies must submit an annual report to DHS on their efforts. DHS serves as the sector-specific agency for 10 of the sectors: information technology; telecommunications; transportation systems; chemical; emergency services; commercial nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities. (See table 1 for a list of sector-specific agencies and a brief description of each sector).

Table 2: Critical TabTable 1: Designated Sector-Specific Agencies and Critical Infrastructure Sectors

Sector-specific agency	Sector	Description
Departments of Agriculture,[a] and Health and Human Services, Food and Drug Administration[b]	Agriculture and food	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production. Carries out the postharvesting of the food supply, including processing and retail sales.
Department of Defense	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 Energy	Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.
Department of Health and Human Services	Public health and health care	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 the Interior	National monuments and icons	Memorializes or represents monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.
Department of the Treasury	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.
Environmental Protection Agency	Drinking water and water treatment systems	Provides sources of safe drinking water from more than 53,000 community water systems and properly treated wastewater from more than 16,000 publicly owned treatment works.

Sector-specific agency	Sector	Description
Department of Homeland Security:		
Office of Infrastructure Protection	Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
	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.
	Dams	Manages water retention structures, including levees, more than 77,000 conventional dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
	Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.
	Commercial nuclear reactors, materials, and waste	Provides nuclear power, which accounts for approximately 20 percent of the nation's electrical generating capacity. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.
Office of Cyber Security and Telecommunications	Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
	Telecommunications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.
Transportation Security Administration	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.
Transportation Security Administration and U.S. Coast Guard	Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Immigration and Customs Enforcement, Federal Protective Service	Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

Source: NIPP, Homeland Security Presidential Directive 7, and the National Strategy for Homeland Security.

[a]The Department of Agriculture is responsible for food (including meat, poultry, and eggs) and agriculture.

[b]The Department of Health and Human Services, Food and Drug Administration is responsible for food and other than meat, poultry, and egg products.

Under the NIPP, the sector-specific agencies, in coordination with their respective government and private sector councils, are responsible for developing individual protection plans for their sectors that, among other things, (1) define the security roles and responsibilities of members of the sector, (2) establish the methods that members will use to interact and share information related to protection of critical infrastructure, (3) describe how the sector will identify its critical assets, and (4) identify the approaches the sector will take to assess risks and develop programs to protect these assets. DHS is to use these individual plans to evaluate whether any gaps exist in the protection of critical infrastructures on a national level and, if so, to work with the sectors to address these gaps.

Sectors Have Established Government and Sector Councils, Which are Generally Representative of their Sectors; Council Activities Have Varied Depending on Their Maturity and Other Characteristics

All of the sectors have established government councils, and voluntary private sector councils under the NIPP model have been formed for all sectors except transportation systems.[7] The nature of the 17 sectors varies and council membership reflects this diversity, but the councils are generally comprised of representatives from the various federal agencies with regulatory or other interests in the sector, some state and local officials with purview over the sectors, and asset owners and operators. Because some of the councils are newer than others, council activities vary based on the council's maturity and other characteristics, with some younger councils focusing on establishing council charters, while more mature councils focused on developing protection strategies.

[7]There is no private sector component for the government facilities sector or the national monuments and icons sector, so these sectors established government councils but not private sector councils.

Some Councils Formed in Response to the NIPP, While Others Formed Earlier because of Increased Vulnerabilities

Seven sectors had not formed either a government council or sector council until after publication of an Interim NIPP in February 2005, while 10 of the sectors had done so. These 10 sectors said they recognized the need to collaborate to address risks and vulnerabilities that could result in economic consequences for their sectors. For example, prior to the development of the NIPP, DHS and the Department of Agriculture had (1) established a government coordinating council for the agriculture and food sector to coordinate efforts to protect against agroterrorism, and (2) helped the agriculture and food sector establish a private sector council to facilitate the flow of alerts, plans, and other information. As of March 2007, the transportation systems sector had yet to form a sector council, but a DHS Infrastructure Protection official said each transportation mode—such as rail, aviation, and maritime—had established a sector council. According to DHS officials, once the modes are organized, the transportation systems council will be formed. Transportation Security Administration (TSA) officials attributed the delay to the heterogeneous nature of the transportation sector—ranging from aviation to shipping to trucking.

Council Leaders Believe That Their Memberships Are Generally Representative of Government Agencies with Purview over the Sectors and Are Generally Representative of Asset Owners and Operators

The composition, scope, and nature of the 17 sectors themselves vary significantly, and the memberships of their government and sector councils reflect this diversity. The enormity and complexity of the nation's critical infrastructure require council membership to be as representative as possible of their respective sectors. As such, council leaders—government sector representatives and private council chairs—believe that their membership is generally representative of their sectors. Government councils include representatives from various federal agencies with regulatory or other interests in the sectors. For example, the chemical sector council includes officials with DHS; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Commerce; the Department of Justice; the Department of Transportation; and the Environmental Protection Agency because each has some interest in the sector. Some government councils also include officials from state and local governments with jurisdiction over entities in the sector.

Private sector council membership varies, reflecting the unique composition of entities within each, but is generally representative of a broad base of owners, operators, and associations—both large and small—within a sector. For example, members of the drinking water and water treatment systems sector council include national organizations such as the American Water Works Association and the Association of Metropolitan Water Agencies and also members of these associations that

are representatives of local entities including Breezy Hill Water and Sewer Company and the City of Portland Bureau of Environmental Services. In addition, the commercial facilities sector council includes more than 200 representatives of individual companies spanning 8 different subsectors, including public assembly facilities; sports leagues; resorts; lodging; outdoor events facilities; entertainment and media; real estate; and retail. This provides the councils opportunities to build the relationships needed to help ensure critical infrastructure protection efforts are comprehensive.

While Newer Councils Are Just Forming, More Mature Councils Are Addressing Long-Term Strategies

Council activities have varied based on the maturity of the councils. Because some of the councils are newer than others, council meetings have addressed a range of topics from agreeing on a council charter to developing industry standards and guidelines for business continuity in the event of a disaster or incident. For example, the commercial facilities government council, which formed in 2005, has held meetings to address operational issues—such as agreeing on a charter, learning what issues are important to the sector, learning about risk management tools, and beginning work on the sector-specific plan. Councils that are more mature have been able to move beyond these activities to address more strategic issues. For example, the banking and finance sector council, which formed in 2002, focused its efforts most recently on strengthening the financial system's ability to continue to function in the event of a disaster or incident (known as "resilience"), identifying a structured and coordinated approach to testing sector resilience, and promoting appropriate industry standards and guidelines for business continuity and resilience.

Good Prior Working Relationships, Willingness to Share Critical Information, and Sufficient Resources Are Key to Council Formation and Progress

Government and sector council representatives most commonly cited long-standing working relationships between entities within their respective sectors and with the federal agencies that regulate them, the recognition among some sector entities of the need to share infrastructure information with the government and within the sector, and operational support from DHS contractors as factors that facilitated council formation. However, these representatives also most commonly identified several key factors that posed challenges to forming some of the councils, including (1) difficulty establishing partnerships with DHS because of issues including high turnover of its staff and DHS staff who lacked knowledge about the sector to which they were assigned, (2) hesitancy to provide sensitive information or industry vulnerabilities to the government due to concerns that the information might be publicly disclosed, and (3) lack of

long-standing working relationships within the sector or with federal agencies.

Recognizing the Need to Work Together; Share Information, and Obtain Support Were Most Common Factors That Helped Facilitate Council Development

One of the factors assisting the formation of many of the government and sector councils was the existence of long-standing working relationships within the sectors and with the federal agencies that regulate them. Ten of the sectors had formed either a government council or private sector council that addressed critical infrastructure protection issues prior to publication of an Interim NIPP. In addition, according to government and sector council representatives, sectors in which the industries have been highly regulated by the federal government—such as the banking and finance sector as well as the commercial nuclear sector—were already used to dealing with the federal government on many issues. Therefore, forming a relationship between the government and the private sector and within the sector was not very difficult.

The availability of DHS contractors that provided administrative and other assistance—such as meeting planning, developing materials, recording and producing minutes, delivering progress reports, and supporting development of governance documents—to the government and sector councils was a third facilitating factor cited by representatives of 13 government and 5 sector councils. For example, representatives of the emergency services sector council and the telecommunications sector council stated that some of the services were very helpful, including guidance the contractors provided on lessons learned from how other sector councils were organized.

Difficulties in Developing Partnerships with DHS, Concerns about Sharing Information, and the Lack of Long-Standing Working Relationships Were the Most Common Challenges to the Formation of Some Councils

Council representatives with three government and eight private sector councils reported that they experienced problems forming their councils due to a number of challenges establishing partnerships with DHS.[8] Specifically, these reported challenges included high turnover of staff, poor communications with councils, staff who were unfamiliar with the sector and did not understand how it works, shifting priorities that affected council activities, and minimal support for council strategies. DHS acknowledged that its reorganization resulted in staff turnover, but according to DHS's Director of the Infrastructure Programs Office within the Office of Infrastructure Protection, this should not have affected formation since DHS has taken a consistent approach to implementing the partnership model and issuing guidance. However, the director acknowledged that continuing staff turnover could affect the eventual success of the partnerships because they are dependent on the interactions and developing trust. Continuity of government staff is a key ingredient in developing trusted relationships with the private sector.

Representatives with six government and five sector councils noted that the private sector continues to be hesitant to provide sensitive information regarding vulnerabilities to the government as well as with other sector members due to concerns that, among other things, it might be publicly disclosed. For example, these representatives were concerned that the items discussed, such as information about specific vulnerabilities, might be subject to public disclosure under the Federal Advisory Committee Act and thereby be available to competitors or potentially make the council members subject to litigation for failure to publicly disclose any known threats or vulnerabilities.[9]

This issue continues to be a long-standing concern and one that contributed to our designating homeland security information sharing as a

[8]As noted earlier, DHS serves as the sector-specific agency for 10 of the sectors: information technology; telecommunications; transportation systems; chemical; emergency services; commercial nuclear reactors, materials, and waste; postal and shipping; dams; government facilities; and commercial facilities. In addition, each government council is co-chaired by a DHS representative.

[9]The Federal Advisory Committee Act (codified at 5 U.S.C. app. 2) was enacted, in part, to control the advisory committee process and to open to public scrutiny the manner in which government agencies obtain advice from private individuals and groups. See 648 F. Supp. 1353, 1358-59 (D.D.C. 1986).

high-risk issue in January 2005.[10] We reported then that the ability to share security-related information is critical and necessary because it can unify the efforts of federal, state, and local government agencies and the private sector in preventing or minimizing terrorist attacks. In April 2006, we reported that DHS continued to face challenges that impeded the private sector's willingness to share sensitive security information with the government.[11] In this report, we assessed the status of DHS efforts to implement the protected critical infrastructure information (PCII) program created pursuant to the Homeland Security Act. This program was specifically designed to establish procedures for the receipt, care, and storage of critical infrastructure information voluntarily submitted to the government. We found that while DHS created the program office, structure, and guidance, few private sector entities were using the program. Challenges DHS faced included being able to assure the private sector that such information will be protected and specifying who will be authorized to have access to the information, as well as to demonstrate to critical infrastructure owners the benefits of sharing the information. We concluded that if DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust that critical infrastructure owners have in the government's ability to use and protect their sensitive information. We recommended that DHS better define its critical infrastructure information needs and better explain how this information will be used. DHS concurred with our recommendations. In September 2006 DHS issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS.

Four government and four sector council representatives stated that the lack of prior working relationships either within their sector or with the federal government created challenges in forming their respective councils. For example, the public health and health care sector struggled with creating a sector council that represented the interests of the sector because it is composed of thousands of entities that are not largely

[10]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005). Since 1990, we have periodically reported on government operations that we have identified as high-risk. In January 2005, we designated information sharing for homeland security as a governmentwide high-risk area because, although information sharing was receiving increased attention, this area still faced significant challenges.

[11]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.: Apr.17, 2006).

involved with each other in daily activities. According to the sector-specific agency representative of the Department of Health and Human Services (HHS), historically, there was relatively little collaboration on critical infrastructure protection-related issues among sector members. Despite these reported challenges, the public health and health care sector has been able to form a sector council that is in the early stages of organization. The commercial facilities sector, which also involves varied and often unrelated stakeholders nationwide, similarly reported that the disparities among stakeholders made forming a council challenging. This sector encompasses owners and operators of stadiums, raceways, casinos, and office buildings that have not previously worked together. In addition, the industries composing the commercial facilities sector did not function as a sector prior to the NIPP and did not have any prior association with the federal government. As a result, this sector council has been concentrating its efforts on identifying key stakeholders and agreeing on the scope of the council and its membership.

Councils Delayed Their Work on Plans until the NIPP Was Issued, but Despite Challenges Submitted Plans to DHS by the Due Date

Each of the 17 sectors provided a sector-specific plan to DHS by the end of December 2006, as required by the NIPP, according to DHS Infrastructure Protection officials. Representatives from both the government and sector councils cited factors that have facilitated the development of their plans—similar to those that facilitated development of their councils—most commonly citing pre-existing plans; historical relationships between the federal government and the private sector or across the private sector, and contractor support. Sector representatives most commonly reported that key challenges in drafting their plans were the late issuance of a final NIPP, which caused some sectors to delay work on their plans, the changing nature of DHS guidance on how to develop the plans, and the diverse make-up of sector membership.

Sector-Specific Agencies Completed Their Plans on Time

Sector-specific agencies met the deadline to complete their plans by December 2006, according to DHS Infrastructure Protection officials. The NIPP requires these plans to contain definitions of the processes the sectors will use to identify their most critical assets and resources as well as the methodologies they will use to assess risks, but not information on the specific protective measures that will be utilized by each sector. The NIPP also requires agencies to coordinate the development of plans in collaboration with their security partners represented by government and sector councils and provide documentation of such collaboration. To date, the level of collaboration between sector-specific agencies and the sector councils in developing the sector-specific plans has varied—ranging from

soliciting stakeholder comments on a draft to jointly developing the plan. For example, TSA developed the transportation systems plan and solicited input from private sector stakeholders, while representatives of the energy sector council worked with the Department of Energy to draft the energy plan. Despite these differences, according to DHS Infrastructure Protection officials, all the sectors submitted their plans to DHS by the December 2006 deadline and DHS and other stakeholders are in the process of reviewing them.

Pre-existing Plans, Collaboration, and Contractor Support Were Factors Most Commonly Cited as Facilitating Development of Sector-Specific Plans

Sector representatives from the agriculture and food, banking and finance, chemical, and energy sectors said their sectors had already developed protection plans prior to the interim NIPP published in February 2005 because they had recognized the economic value in planning for an attack. These representatives said they were able to revise their previous plans to serve as the plans called for in the NIPP. For example, the Department of Energy, with input from the sector, had developed a protection plan in anticipation of the Year 2000 computer threat; Department of Energy officials noted that both this plan and the relationships established by its development have been beneficial in developing the protection plan for the energy sector. Similarly, the banking and finance sector council, which worked closely with the Department of Treasury, has had a critical infrastructure protection plan in place for the banking and finance sector since 2003 and planned to use it, along with other strategies, to fit the format required by the NIPP.

Representatives from 13 government and 10 sector councils agreed that having prior relationships—either formally between the federal government and the private sector based on regulatory requirements, or informally within and across industries—facilitated sector-specific plan development. For example, a nuclear sector representative said that its regulator, the Nuclear Regulatory Commission, had already laid out clear guidelines for security and threat response that facilitated developing the sector's plan. The drinking water and wastewater sector council representative said that its long-standing culture of sharing information and decades of work with the Environmental Protection Agency helped with plan development.

Representatives from seven sector-specific agencies and five sector councils said that assistance from DHS officials or DHS contractors was also a factor that helped with plan development, such as research and drafting. For example, DHS contract staff assisted the Department of the Interior and DHS's Chemical and Nuclear Preparedness and Protection

Division in drafting the plans for the national monuments and icons and emergency services sectors, respectively. Representatives from the chemical, emergency services, nuclear, and telecommunications sector councils said that contractors hired by DHS were helpful as resources providing research or drafting services.

The Late Issuance of a Final NIPP, Changing Guidance, and Other Challenges Impeded Progress on Some Sector-Specific Plans

Representatives from six government councils and six sector councils said that the delays in issuing a final NIPP and changing DHS sector-specific plan guidance contributed to delays in developing their sector plans. According to DHS, sectors had begun drafting their sector-specific plans following the issuance of initial plan guidance in April 2004. But, DHS issued revised guidance based, in part, on stakeholder comments a year later with new requirements, including how the sector will collaborate with DHS on risk assessment processes as well as how it will identify the types of protective measures most applicable to the sector. DHS then issued additional guidance in 2006 requiring that the plans describe how sector-specific agencies are to manage and coordinate their responsibilities. These changes required some sectors—such as dams, emergency services, and information technology—to make significant revisions to their draft plans. Representatives from these sectors expressed frustration with having to spend extra time and effort making changes to the format and content of their plans each time DHS issued new guidance. Therefore, they decided to wait until final guidance was issued based on the final, approved NIPP. In our current work, once we have access to these plans, it will be important to determine how these delays may have affected the quality, completeness, and consistency of the plans.

However, some sectors found the changes in the NIPP and plan guidance to be improvements over prior versions that helped them prepare their plans. For example, representatives from the emergency services sector said that guidance became more specific and, thus, more helpful over time, and representatives from the national monuments and icons sector said that the DHS guidance has been useful. Representatives from the information technology, public health, energy, telecommunications, and transportation systems sectors, among others, had commented that the NIPP should emphasize resiliency—meaning how quickly can a key asset or resource begin operations after an incident—rather than protection measures, such as hiring guards, installing gates and similar actions. According to some of these representatives, it is impossible and cost-prohibitive to try to protect every asset from every possible threat. Instead, industries in these sectors prefer to invest resources in protecting

the most critical assets with the highest risk of damage or destruction and to plan for recovering quickly from an event. Representatives from the telecommunications sector added that resiliency is especially important for interdependent industries in restoring services such as communications, power, the flow of medical supplies, and transportation as soon as possible. DHS incorporated the concept of resiliency into the final NIPP to address these concerns and continues to emphasize protection as well.

As in establishing their councils, in developing their sector-specific plans, officials from three government councils and five sector councils said that their sectors were made up of a number of disparate stakeholders, making agreement on a plan more difficult. For example, the commercial facilities sector is composed of eight different subsectors of business entities that have historically had few prior working relationships. According to the government council representative, the magnitude of the diversity among these subsectors has slowed the process of developing a plan so that the sector only had an outline of its plan as of May 2006. Similarly, government and private council representatives of the agriculture and food sector indicated that the diversity of industries included in this sector such as farms, food-processing plants, and restaurants, each of which has differing infrastructure protection needs, has made developing a plan more difficult.

DHS Needs to Fulfill Key Cybersecurity Responsibilities and Address Challenges and GAO Recommendations

To some extent, all sectors depend on cyber infrastructure to operate, such as using computers to control access at nuclear facilities. So, it is important that sectors include cybersecurity in their sector's protection plan and programs. 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. Specifically, in 2005, we reported that DHS had initiated efforts to fulfill 13 key cybersecurity responsibilities (shown in table 2), 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 NIPP—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 time frames for completion and the relationships among its various initiatives are not evident.

Table 2: Thirteen DHS Cybersecurity Responsibilities

Responsibilities	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.
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.

Responsibilities	Description
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.

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. In addition, we reported that DHS faced a particular challenge in attaining the organizational stability and leadership it needed to gain the trust of other stakeholders in the cybersecurity world—including other government agencies as well as the private sector.

In July 2005, DHS undertook a reorganization that established the position of the Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. In September 2006, DHS announced the appointment of an Assistant Secretary for Cyber Security and Telecommunications. Since the appointment, the Assistant Secretary has led efforts to ensure the inclusion of cybersecurity in each critical infrastructure sector's sector specific plan. The Assistant Secretary has set priorities that include (1) preparing for and deterring attacks by encouraging entities, through implementation of the sector specific plans, to systematically assess their network vulnerabilities and take steps to fix them, (2) responding to cyber attacks of potentially national significance by leveraging operational expertise and building situational awareness and incident response capabilities of the government and private sector; and (3) building awareness about the responsibilities for securing networks across the public and private sectors.

In addition to the National Cyber Security Division, the Assistant Secretary is also responsible for the National Communications System, which ensures continuity of communications and priority service for the government under conditions of national emergency, and the Office of Emergency Communications, established pursuant to the fiscal year 2007

DHS appropriations act.[12] This office is responsible for developing a national strategy and technical assistance and outreach to state and local governments for ensuring operable and interoperable emergency communications capabilities for first responders.

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. DHS concurred with most of the recommendations addressed to them. Together, the recommendations provide a high-level road map for DHS to use in working to improve our nation's cybersecurity posture. While DHS has made progress in addressing some of these recommendations many things remain to be done. 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. Table 3 shows our detailed recommendations.

[12] Pub. L. No. 109-295, § 671(b), 1355, 1433-41 (2006).

Table 3: Key GAO 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 section 1016 of the Intelligence Reform and Terrorism Prevention Act, assess progress toward the milestones set in the Interim Implementation Plan for the Information Sharing Environment; 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.[a]
	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 Information Sharing and Analysis Centers (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.

Functional area	Recommendations that have not yet been fully implemented
	Considering the roles, responsibilities, and actions established in the information-sharing plan, develop appropriate DHS policies and procedures for interacting with the ISACs, sector coordinators, and sector-specific agencies and for coordination and information sharing.
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, GAO-01-323.

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

Concluding Observations

Critical infrastructure protection is vital to our national security, economic vitality, and public health. Yet a decade after focusing on improving our ability to protect our key assets and resources, progress has been mixed, as Katrina demonstrated. It showed that significant damage to critical infrastructure and key resources could disrupt the functioning of businesses and government alike, underscoring the need for the private and public sector to establish stronger partnerships and working relationships in order to take a coordinated approach to critical infrastructure protection. DHS has moved out by issuing the National

Infrastructure Protection Plan as a guiding framework for a national effort, and is providing contractor, technical, and analytical support to sectors, among other things, to encourage progress. Likewise, some sectors—those who are more mature, have been regulated, are more homogeneous, or had economic incentives, such as the threat of Y2K—came together to collaborate, work effectively, and develop protection strategies, even before DHS established the national plan. But other sectors—those who have just been created, who have not worked with federal agencies in the past, who are not regulated but must volunteer to participate in the planning process, and who are large and diverse—face bigger challenges in achieving this coordination and rate of progress. Despite these challenges, each sector submitted a protection plan to DHS. However, DHS has yet to release them. Given the wide variance in the maturity of the sectors, the quality, comprehensiveness, completeness, and consistency of the plans remain to be seen. In addition, it is important to realize that in some cases, the sector specific plan is really more of a first step—a "plan to plan." In other words, the sectors were only to describe how they expect to identify and prioritize critical assets, how they expect to assess their risks, vulnerabilities, threats and consequences, and how they will approach developing protection programs, not detail how they will implement them.

Thus, fulfilling its statutory responsibilities for ensuring the nation's critical infrastructure is protected will be a long-term commitment for DHS. This makes it even more important that DHS address challenges that our work has identified over the years and for which we have made a number of recommendations yet to be implemented, including our body of work assessing the protection of cyber infrastructure. These challenges include building trusted working relationships and better collaborating with states and localities, given that the infrastructure is in their communities, as well as the private sector, given that they own most of the assets and resources. Challenges also include providing the environment and incentives for the private sector to voluntarily share information with DHS on gaps in vulnerabilities and protective measures, information that the agency must have to be able to ensure assets and resources critical to the nation are protected. Challenges also include providing organizational stability and leadership, addressing employee turnover and gaps in expertise, and enhancing agency capabilities, such as for providing analysis and warning and identifying and assessing threats and vulnerabilities.

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

Contact Information

For further information on this testimony, please contact Eileen Larence at (202) 512-8777 or by e-mail at larencee@gao.gov, or regarding cyber-critical infrastructure protection issues, David Powner at (202) 512-9286 or by e-mail at pownerd@gao.gov. Individuals making key contributions to this testimony include Susan Quinlan, Assistant Director; Michael Gilmore; Landis Lindsey; and Edith Sohna.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548