United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2006

CRITICAL INFRASTRUCTURE PROTECTION

Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics

GAO-07-39

October 2006

CRITICAL INFRASTRUCTURE PROTECTION

Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-39, a report to congressional requesters

Why GAO Did This Study

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures and key resources 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).

GAO examined (1) the extent to which these councils have been established; (2) the key facilitating factors and challenges affecting the formation of the councils; and (3) the overall status of the plans and key facilitating factors and challenges encountered in developing them. GAO obtained information by reviewing key documents and conducting interviews with federal and private sector representatives.

GAO is not making any recommendations at this time since prior recommendations are still being implemented. Continued monitoring will determine whether further recommendations are warranted.

www.gao.gov/cgi-bin/getrpt?GAO-07-39.

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

All 17 critical infrastructure sectors have established their respective government councils, and nearly all sectors have initiated their voluntary private sector councils in response to the NIPP. However, council activities have varied due to council characteristics and level of maturity. 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 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 formation. For example, long-standing working relationships with regulatory agencies and within sectors were frequently cited as the most helpful factor in establishing councils. 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.

At the time of GAO's review, all of the sectors were preparing plans, although these plans were at varying stages of completion—ranging from nearly complete to an outline. Nevertheless, all sectors expected to submit their plans to DHS by the December 2006 deadline. DHS's 18-month delay in issuing the NIPP and the changing nature of DHS guidance on sector plans were cited as challenges to developing the plans. As of August 2006, collaboration between the sector and government councils on the plans, which is required by the NIPP, had yet to take place for some sectors. Issuing the NIPP and completing sector plans are only first steps to ensure critical infrastructure is protected. More remains to be done to ensure the adequate protection of our nation's critical infrastructure. A number of sectors still need to identify their most critical assets across their sectors, assess their risks, and agree on protective measures.

DHS, the Department of Health and Human Services, and the Environmental Protection Agency had no formal comments on the draft report but provided technical comments.

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
FACA	Federal Advisory Committee Act
GMU	George Mason University
HHS	Department of Health and Human Services
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network Critical Sectors
HSPD-7	Homeland Security Presidential Directive 7
HSPD-9	Homeland Security Presidential Directive 9
ISAC	information sharing and analysis center
NIPP	National Infrastructure Protection Plan
PCII	protected critical infrastructure information
PCIS	Partnership for Critical Infrastructure Security
PDD-63	Presidential Decision Directive 63
TSA	Transportation Security Administration

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 16, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Todd Platts
Chairman
Subcommittee on Government Management, Finance and Accountability
Committee on Government Reform
House of Representatives

The Honorable Bennie G. Thompson
Ranking Minority Member
Committee on Homeland Security
House of Representatives

The Honorable Robert F. Bennett
United States Senate

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 detailed surveillance of the New York Stock Exchange and the Citigroup Center in the laptop computer of an Al Qaeda operative captured in Pakistan, part of a plan to target financial institutions in New York. Moreover, a series of coordinated suicide bombings in 2005 that struck London's public transportation system demonstrated how an attack on the transportation system could disrupt a 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] Among other requirements, the Homeland Security 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 defines 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. Among other responsibilities, the Secretary of Homeland Security 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 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.

Consistent with the Homeland Security Act, HSPD-7 required DHS to develop a comprehensive and integrated plan by December 2004 that outlines national goals, objectives, milestones, and key initiatives necessary to fulfilling these responsibilities. In response, DHS developed a 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

[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; 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 healthcare; 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.

protection activities within and across sectors in an integrated, coordinated fashion. The NIPP also requires the individual sector-specific agencies to submit plans to DHS by the end of December 2006 detailing the application of the national plan's core elements to each of their respective sectors. These individual plans are to establish the means by which the sectors will identify critical assets within the sector, 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. These plans are to be developed by the designated federal sector-specific agencies in coordination with relevant government and private-sector representatives and are, among other things, to address the unique characteristics and risks of each 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 them. While the NIPP establishes a deadline for the submission of these plans, DHS anticipates that the NIPP and sector-specific plans will continue to evolve as the critical infrastructures, threats against them, and strategies for protecting and responding to these threats and incidents evolve.

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)—comprised of federal, state, local, or tribal agencies with purview over critical assets—and encourages voluntary formation of sector coordinating councils (sector councils)—comprised of owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations. These councils create the structure through which representative groups from all levels of government and the private sector are to collaborate in planning and implementing efforts to protect critical infrastructure. The sector councils are envisioned to be policy-related and to represent a primary point of contact for government to plan the entire range of infrastructure protection activities unique to the sector. These functions are distinct from those of the private sector's information sharing and analysis centers (ISACs) that were previously established to serve as mechanisms for gathering, analyzing, and disseminating information on infrastructure threats and vulnerabilities to and from private infrastructure sectors and the government but are not to serve as policy-making bodies. These councils also are to collaborate with the sector-specific agencies in the development and review of their respective individual sector plans.

In response to your request to determine the extent to which DHS has developed a strategy to identify, prioritize, and coordinate the protection of critical infrastructure, including how the department intends to work with other federal departments and agencies, state and local governments, and the private sector to develop this strategy, our objectives were to

- determine the extent to which government and sector councils have been established for each sector and compare their general characteristics;
- identify the key facilitating factors and challenges that critical infrastructure protection stakeholders encountered in establishing their respective councils; and
- ascertain the status of individual sector-specific plans and the key facilitating factors and challenges that critical infrastructure protection stakeholders encountered in developing their plans thus far.

To address these objectives, we reviewed our prior work that focused on government and private sector critical infrastructure protection coordination efforts as well as related studies by others. (See "Related GAO Products" at the end of this report for a list of our prior work). We reviewed the interim, draft, and final versions of the NIPP as well as sector-specific plan guidance, to determine council roles and responsibilities and requirements for individual sector-specific plans. We also conducted structured interviews to determine the status of the government councils and individual sector-specific plans with designated representatives of each of the sector-specific agencies with critical infrastructure protection responsibility for the 17 critical infrastructure sectors: DHS,[3] the Department of Agriculture, the Department of Health and Human Services, the Department of Defense, the Department of Energy, the Department of the Interior, the Department of the Treasury, and the Environmental Protection Agency. We also conducted structured interviews with the chairs, co-chairs, or steering committee

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

representatives of each of the 14 sector councils[4] that are part of the NIPP framework and a representative of the Rail Sector Coordinating Council to determine the status of the councils and the sector-specific plans. These officials also presented their views on the facilitating factors and barriers to creating and maintaining their respective councils and drafting sector-specific plans, but they did not necessarily represent the views of each member of the councils. For both the government and sector council contacts, the structured interviews solicited information including (1) the status of council formation, leadership, organization, and goals; (2) views on whether specific factors facilitated or impeded council formation; (3) the status of sector-specific plan development; and (4) views on whether specific factors facilitated or impeded plan development. We also spoke with the Deputy Director, Infrastructure Partnerships Division and the Director of the Infrastructure Programs Office within DHS's Office of Infrastructure Protection about the formation of the councils and the development of sector-specific plans.[5] We conducted our work from October 2005 through August 2006 in accordance with generally accepted government auditing standards.

Results in Brief

Each of the infrastructure sectors has established government councils, and voluntary sector councils have been formed in response to the recommended NIPP partnership model for all sectors except transportation systems. The characteristics and levels of maturity vary significantly across the sectors. 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 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. For example, members of the drinking water and water treatment systems sector council included the American Water Works Association as well as local

[4]The government facilities sector and the national monuments and icons sector do not have sector councils because they have no private sector components.

[5]DHS's Office of Infrastructure Protection is to identify and assess current and future threats to the nation's physical and informational infrastructure and to issue warnings to prevent damage to the infrastructure that supports community and economic life. It is also responsible for oversight of NIPP development and implementation of the partnership model.

entities, such as the City of Portland Bureau of Environmental Services. According to representatives from several sector councils, these councils are not intended to replace the information sharing functions provided by the information sharing and analysis centers, and two of the centers are members of their respective sector 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. The transportation systems sector had yet to form a sector council and, as of August 2006, Transportation Security Administration officials said they were working with contractors to help each transportation mode establish its own sector council. According to DHS officials, once the modes are organized the transportation systems sector 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. Our past work has also identified trusted working relationships and effective information sharing as critical factors for successful public-private partnerships, and we have made recommendations in these areas that DHS

generally agreed with, but has yet to fully implement.[6] 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. For example, one of the contractors provided guidance on lessons learned in how other sector councils were organized that representatives of the emergency services and the telecommunications councils said were very helpful. 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, 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. To address this concern about public disclosure of sensitive information and to enhance information sharing, in March 2006 DHS created the Critical Infrastructure Partnership Advisory Council—open to members of all councils—that is exempt from the Federal Advisory Committee Act,[7] but it is too soon to determine if this council has promoted more sharing.

As of August 2006, each of the 17 sector-specific agencies was in the process of preparing a sector-specific plan to demonstrate how that sector will comply with the NIPP. However, the sectors were at varying stages of completion in developing their plans, ranging from almost complete to having only completed an outline. For example, the chemical and nuclear

[6]See GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection.* GAO-02-24 (Washington, D.C.: Oct.15, 2001); *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 (Washington, D.C.: June 16, 2006).

[7]The Federal Advisory Committee Act (FACA) (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). Pursuant to authority conferred by the Homeland Security Act, 6 U.S.C. § 451, DHS established the Critical Infrastructure Partnership Advisory Council as a FACA exempt body to support the free flow of information and the need for regular, interactive discussions concerning threats and vulnerabilities. See 71 Fed. Reg. 14,930 (Mar. 24, 2006).

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, all the sectors expected to submit initial plans to DHS by the December 2006 deadline. 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 the risks posed to it, but DHS guidance does not require the plans to address how the sector is actually assessing risk and protecting its most critical assets. Council members cited as a key facilitating factor the existence of 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 lack 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. For example, DHS revised its initial 2004-plan guidance after a year with new requirements including how the sectors will collaborate with DHS on risk assessment processes. DHS then issued additional guidance in 2006 that required the plans to have a new chapter describing how sector-specific agencies are to manage and coordinate their responsibilities. Several council members said it was frustrating to have to update their protection plans in response to changes from the interim, the draft, and the final NIPP, even though DHS made some of these changes 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. Finally, several cited the heterogeneous characteristics of some sectors, such as the different industries that make up the agriculture and food sector, as making collaboration and consensus on their plans a challenge. While DHS has made progress with some critical infrastructure challenges, until it addresses our already outstanding recommendations, it will have difficulty achieving results in its role as a federal focal point for critical infrastructure. Because our findings in this report echo many of those in our previous reports and are covered by previous recommendations to DHS that have yet to be fully implemented, we are not making any new recommendations at this time. Continued monitoring will determine whether further recommendations are warranted.

DHS, the Department of Health and Human Services, and the Environmental Protection Agency had no formal comments on the draft report, but they provided technical comments that we used to clarify the report as appropriate.

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. Several federal policies address the importance of coordination between the government and the private sector in critical infrastructure protection. 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 the physical and cyber-based systems essential to the minimum operations of the economy and the government. Among other things, this directive designated government agencies to coordinate and support critical infrastructure protection efforts and identified lead federal agencies to work with coordinators in eight infrastructure sectors and five areas called special functions at the time. The directive also encouraged development of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and disseminating information on infrastructure threats and vulnerabilities to and from private infrastructure sectors and the federal government. (See table 1 for a list of functional ISACs).

Table 1: Operating ISACs, as of July 2006

Sector	ISAC	ISAC Established
Agriculture and food	Food	Feb. 2002
Banking and finance	Financial Services	Oct. 1999
Chemical	Chemical	April 2002
Commercial facilities	Real Estate	Feb. 2003
Drinking water and water treatment systems	Water	Dec. 2002
Emergency services	Emergency Management and Response	Oct. 2000
Energy	Electric	Oct. 2000
	Energy	Nov. 2001
Government facilities	Multi-State	Jan. 2003
Information technology	IT	Dec. 2000
	Research & Education Network	Feb. 2003
Telecommunications	National Coordinating Center for Telecommunications	Jan. 2000
Transportation systems	Public Transit	Jan. 2003
	Surface Transportation (rail)	May 2002
	Highway	Mar. 2003
	Maritime	Feb. 2003

Source: Government council and sector council representatives and prior GAO reports.

Note: The following critical sectors do not have ISACs: dams; defense industrial base; national monuments and icons; commercial nuclear reactors, materials, and waste; postal and shipping; and public health and healthcare.

In December 2003, Homeland Security Presidential Directive 7 (HSPD-7) was issued, superseding PDD-63. HSPD-7 defined responsibilities for DHS, federal agencies that are responsible for addressing specific critical infrastructure sectors—sector-specific agencies,—and other departments and agencies. HSPD-7 instructs these sector-specific agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. HSPD-7 makes DHS responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. HSPD-7 requires DHS to (1) produce a national plan summarizing initiatives for sharing information, including providing threat warning data to state and local governments and the private sector and (2) establish the appropriate systems, mechanisms, and procedures to share homeland security information (including information on critical infrastructure

protection such as threat-warning data) with other federal departments and agencies, state and local governments, and the private sector in a timely manner. According to the NIPP, additional DHS responsibilities regarding critical infrastructure protection include developing and implementing comprehensive risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance; recommending risk management and performance criteria and metrics within and across sectors; and establishing structures to enhance the close cooperation between the private sector and government at all levels. (For additional key federal initiatives related to critical infrastructure protection, see app. I).

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

HSPD-7 designated sector-specific agencies for each of the critical infrastructure sectors. These federal agencies are responsible for infrastructure protection activities in their assigned sectors, which include coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector to carry out sector protection responsibilities. These activities also include facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. HSPD-7 also requires that these agencies submit an annual report to DHS on their efforts to identify, prioritize, and coordinate the protection of critical infrastructures in their respective sectors. DHS serves as the sector-specific agency for ten 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 2 for a list of each sector-specific agency and a brief description of each sector).

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

Sector-specific agency	Sector	Description
Dept. of Agriculture[a] Dept. of Health and Human Services, Food and Drug Administration[b]	Agriculture & 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.
Dept. 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.
Dept. 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.

Sector-specific agency	Sector	Description
Dept. of Health and Human Services	Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.
Dept. 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.
Dept. 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.
Dept. 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% 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.

Sector-specific agency	Sector	Description
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 U.S. 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 other than meat, poultry, and egg products.

Under the NIPP, the sector-specific agencies are also responsible for developing individual plans for their sectors. These plans are to support the NIPP by identifying the specific protective activities and information-sharing mechanisms and protocols that each sector will be using for its protection efforts. Specifically, these plans are to be tailored to address the unique characteristics and risks of each sector and are to, 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 them. Each sector-specific agency is to collaborate with its respective government and sector councils to develop these plans, and each is to submit its plan to DHS within 180 days of issuance of the NIPP (by the end of December 2006).

NIPP Relies on a Partnership Model for Coordination of Protection Efforts

DHS published an Interim NIPP in February 2005 that was intended to provide the framework for a coordinated national approach to address the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructure. DHS released subsequent drafts of the NIPP for comment in November 2005 and January 2006 before it released a final NIPP in June 2006. The NIPP relies on a sector partnership model as the primary means of coordinating government and private sector critical infrastructure protection efforts. Under this model, each sector has both a government council and a sector council to address sector-specific planning and coordination. Each council is to work in tandem to create the context, framework, and support for coordination and information-sharing activities required to implement and sustain that sector's critical infrastructure protection efforts. The council framework allows for the involvement of representatives from all levels of government and the private sector, so that collaboration and information-sharing can occur to assess events accurately, formulate risk assessments, and determine appropriate protective measures.

The government councils are to coordinate strategies, activities, policy, and communications across government entities within each sector. Each government council is to be comprised of representatives across various levels of government (i.e., federal, state, local, and tribal) as appropriate to the security needs of each individual sector. In addition, a representative from the sector-specific agency is to chair the council and is to provide cross-sector coordination with each of the member governments. Each council is also co-chaired by the DHS Assistant Secretary for Infrastructure Protection or a designee.

Sector councils are encouraged under the NIPP model to be the principal entities for coordinating with the government on a wide range of critical infrastructure protection activities and issues. Under the model, critical asset owners and operators are encouraged to be involved in the creation of sector councils that are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership.[8] Specific membership can vary from sector to sector, but should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within the sector.

[8] Owners and operators of these assets include private sector entities and, in some cases, state and local governments.

The NIPP also identified cross-sector entities that are to promote coordination, communications, and the sharing of key practices across sectors. On the government side, the Government Cross-Sector Council is comprised of two subcouncils: (1) the NIPP Federal Senior Leadership Council, comprised of representatives of each of the sector-specific agencies, that is to enhance communication and coordination between and among these agencies and (2) the State, Local, and Tribal Government Coordinating Council—comprised of state, local, and tribal homeland security advisors—that is to serve as a forum for coordination across these jurisdictions on protection guidance, strategies, and programs. On the private sector side, the Partnership for Critical Infrastructure Security (PCIS), comprised of one or more members and alternates from each of the sector councils, is to, among other things, provide senior-level, cross-sector strategic coordination through partnership with DHS and the sector-specific agencies and to identify and disseminate protection best practices across the sectors.

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 sector councils under the NIPP model have been formed for all sectors except transportation systems. These councils were formed as early as 2002 to as recently as 2006. The nature of the 17 sectors varies and council membership reflects this diversity. The government councils are generally comprised of representatives from various federal agencies with regulatory or other interests in the sector as well as some state and local officials with purview over the sectors. In addition, members of the sector councils are generally representative of the asset owners and operators within the sectors. 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.

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

Each of the 17 critical infrastructure sectors has established its government council, and sector councils have been formed for all sectors except transportation systems.[9] While seven sectors did not form either a government council or sector council prior to the drafting of the NIPP, ten of the sectors had formed at least one of these councils prior to DHS's drafting of the NIPP. These sectors said they recognized the need to collaborate to address risks and vulnerabilities that could result in economic consequences for their sectors. The sectors with pre-existing councils are generally using them to serve as the councils laid out in the NIPP model. For example, prior to the development of the NIPP, DHS and the Department of Agriculture established a government coordinating council for the agriculture and food sector to coordinate efforts to protect against agroterrorism. Also, prior to NIPP development, DHS helped the agriculture and food sector establish a sector council to facilitate the flow of alerts, plans, and other information between federal and state governments and private infrastructure groups. The transportation systems sector had yet to form a sector council, and, at the time of our review, Transportation Security Administration officials said they were working with contractors to help each transportation mode establish its own sector council. TSA officials attributed the delay to the heterogeneous nature of the Transportation sector—ranging from aviation to shipping to trucking. (See table 3 for the status of government and sector council formation by sector).

[9]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.

Table 3: Status of Government Council and Sector Council Formation, as of August 2006

Sector	Government council formed	Sector council formed
Agriculture and food	2003	June 2004
Banking and finance	January 2002	June 2002
Chemical	March 2005	June 2004
Commercial facilities	Summer 2005	Fall 2005
Commercial nuclear reactors, materials, and waste	October 2004	September 2004
Dams	January 2005	May 2005
Defense industrial base	July 2006	August 2006
Drinking water and water treatment systems	April 2005	September 2004
Emergency services	April 2005	July 2003
Energy[a]	Spring 2004	June 2004
Government facilities	November 2005	Not applicable[b]
Information technology	April 2005	January 2006
National monuments and icons	September 2005	Not applicable[b]
Postal and shipping	July 2005	December 2004
Public health and healthcare	Pre-2005	Initiated in 2003, reorganized in 2006
Telecommunications	May 2005	May 2005
Transportation systems	January 2006	Not formed

Source: Government council and sector council representatives.

[a]The energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[b]There is no private sector component to this sector.

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 the entities that make up the respective sector and that are responsible for or have some role in protecting them. As such, council leaders—government sector representatives and private council chairs—believe that their membership is generally representative of their sectors. In terms of government councils, members are generally comprised of representatives from various federal agencies with regulatory or other interests in the sectors (see app. II for government council membership by sector). For example, the chemical sector government council membership 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. This is because each entity has an interest in some form in the chemical sector. As permitted in the NIPP model, some government councils also include officials from state and local governments with jurisdiction over entities in the sector. An example of this is the dams sector, in which its government council includes not only federal officials with purview over the sector but also state officials from the California Department of Water Resources; the New Jersey Department of Environmental Protection; the Ohio Department of Natural Resources; the Virginia Department of Conservation and Recreation; and the Washington Department of Ecology. These states represent the other states and all local governments in their regions. According to agency representatives for each of the government councils, the memberships may change over time if needed—for example, if knowledge of new threats would require the involvement of additional government entities.

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 (see app. III for sector council membership by 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. According to sector council representatives, memberships generally represent the majority of private industries within each sector. This provides the councils opportunities to build the relationships needed to help ensure critical infrastructure protection efforts are comprehensive. The two exceptions are the transportation systems sector council and the public health and healthcare sector council. According to government and sector representatives, because the transportation systems sector has yet to establish a council, memberships are yet to be determined. Because of the vast number of business entities within the private sector that are very diverse in their interests, it has been difficult for the public health and healthcare sector council to engage a mix of critical asset owners that everyone considers representative. There are a large number of public

health and healthcare organizations involved in the sector that do consider themselves representative of the market. According to DHS's Director of the Infrastructure Programs Office within the Office of Infrastructure Protection, owners and operators are necessary members of the council because they have the responsibility to invest time, money, and other resources to secure their critical assets and are held responsible by their customers and by the public they serve to respond and recover when their operations are disrupted. Recently, a new public health and healthcare chair of the sector council has been designated and is working to solidify the council's structure and membership. While these efforts may help, it is unclear how soon this will happen.

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.

Sector councils are not intended to replace the information sharing functions provided by the ISACs. For those sectors that had established ISACs prior to the development of the NIPP, the sectors may continue to rely on them for operational and tactical capabilities for information sharing, such as threat alerts, and, in some cases, support for incident response activities. In contrast, sector councils are to serve as strategy and policy-making bodies for critical infrastructure protection. The NIPP also supports the continued use of ISACs by those sectors that have established them, but notes that each sector has the ability to implement a tailored information sharing solution that may include existing ISACs or other methods, such as trade associations, security organizations, or infrastructurewide or corporate operations centers. In fact, the ISACs for the banking and finance sector as well as the information technology

sector are members of their respective sector councils. Many sectors are exploring a relatively new DHS information sharing mechanism, the Homeland Security Information Network (HSIN). This network, in particular the portal for critical infrastructure protection called Critical Sectors (HSIN-CS), is a suite of tools that sector councils can use for information sharing, coordination, and communication about alerts, incidents, and planning efforts within the sector. At the time of our review, according to DHS's Director of the Infrastructure Programs Office within the Office of Infrastructure Protection, DHS had created access portals for all 17 sectors and 6 sector councils had signed formal memorandums of understanding with DHS to use the system, declaring the councils' intent to implement access and use for their entire sector. Once HSIN-CS is fully deployed, some sectors may use it instead of developing separate ISACs or as a supplement to an existing ISAC.

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. As noted earlier in this report, ten of the sectors had formed either a government council or sector council that addressed critical infrastructure protection issues prior to DHS's development of the NIPP. These sectors generally had ready-made councils in terms of the NIPP model, compared to sectors that did not have prior relationships. 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. For example, the banking and finance sector has had a functional equivalent of both the government and sector councils since 2002 as well as an ISAC since 1999. Government and sector council representatives reported that members of both councils have developed long-standing and trusted working relationships between respective members of each council and across the two councils and an effective means of information sharing via their ISAC. As we reported in 2001, developing trusted relationships among their members was one of four key factors critical to the success of information sharing organizations in addressing cyber infrastructure threats.[10] We reported that trust was critical to overcome members' reluctance to disclose their weaknesses, vulnerabilities, and other confidential or proprietary business information, but that trust had to be built over time and through personal relationships.

The private sector's recognition of the need to share information with the government about security threats, infrastructure vulnerabilities, and protective measures also helped with council formation, according to representatives of government and sector councils in 15 of the sectors. This recognition dates back to PDD-63 with the formation of the ISACs between 1999 and 2003 and continues today. As we reported in July 2004, the private sector recognized the need to share information with the federal government and many sectors voluntarily created ISACs to provide an appropriate system to do so.[11] Information sharing can communicate both actionable information on threats and incidents as well as information about the overall protection status of critical assets so that owners and operators, federal agencies, states, localities, tribal governments, and others can assess risks, make appropriate security investments, and take effective and efficient protective actions. Government and sector representatives generally see the formation of the councils as another step to improve information sharing between the federal government and the private sector that can ultimately lead to more

[10]GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct.15, 2001).

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

efficient and effective investments by owners and operators as they protect their infrastructure.

The availability of DHS contractors that provided administrative and other assistance to the government and sector councils was a third facilitating factor cited by representatives of 13 government and 5 sector councils. DHS entered into contracts with the following three organizations[12] to provide administrative and other assistance to help fill resource and skill gaps for the councils:

- DHS contracted with VSE Corporation, an engineering and technical support services firm, in September 2005. Under this contract, Energetics, a subcontractor, was to provide support to any of the sectors that requested assistance in developing a common vision for their sector-specific plans. Under this same contract, Meridian Institute, a subcontractor to Energetics, was to provide support to any sector councils that requested help to convene their councils and to build consensus on a governance structure. This contract also supported development of reports and studies related to the partnership model and information sharing with the sectors. According to the most currently available data, VSE-Energetics was provided $3 million for September 2005 to September 2006.

- DHS contracted with SRA International, Inc., in January 2004 to provide "secretariat" support to the government councils. This support was to include meeting planning, logistics, minutes, record keeping, and administrative support. This contract also supported the National Infrastructure Advisory Council, a presidential advisory committee, with administrative, research, and technical writing support. A number of study and analysis efforts were also supported under this contract. SRA was provided $7.8 million from January 2004 to August 2006.

- DHS contracted with George Mason University (GMU) in October 2004 to provide administrative and other support to the Partnership for Critical Infrastructure Security (PCIS) and those sector councils that request support. GMU was provided $2.2 million for October 2004 to December 2006.

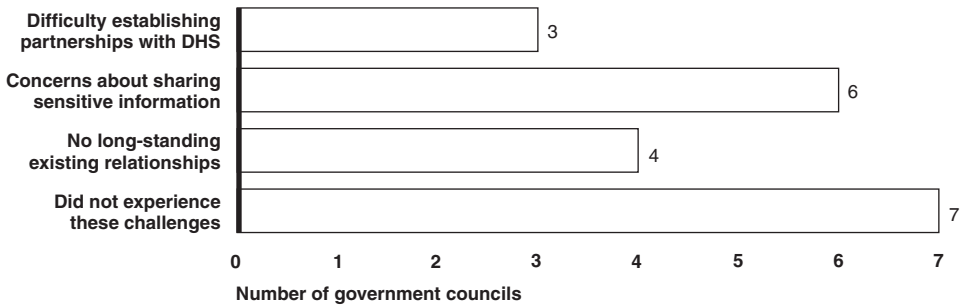
[12]According to DHS officials within its Office of Infrastructure Protection, as of July 2006, it was in the process of re-bidding the support services for all councils.

The council representatives generally viewed these contractors as invaluable in providing administrative, meeting-arrangement, and meeting-facilitation services to the councils. For example, DHS's contract with GMU was to provide meeting-planning, facilitation and logistics support, develop materials, record and produce minutes, deliver progress reports, and support development of governance documents, if requested by the sector councils. Representatives of the emergency services sector council and the telecommunications sector council commended the services GMU provided for being very helpful, including guidance GMU's staff 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

While not all government and sector council representatives cited any particular challenges to forming their councils, those who did mentioned several key factors that included (1) difficulty establishing partnerships with DHS because of issues including high turnover of its staff and lack of staff knowledgeable about their sector; (2) hesitancy to provide sensitive information or industry vulnerabilities to the government or to other sector representatives due to concerns that it might be publicly disclosed; and (3) lack of long-standing working relationships within the sector or a close association with federal agencies. (See figures 1 and 2 for information on the number of councils that listed key factors that posed challenges for government and sector councils, respectively).

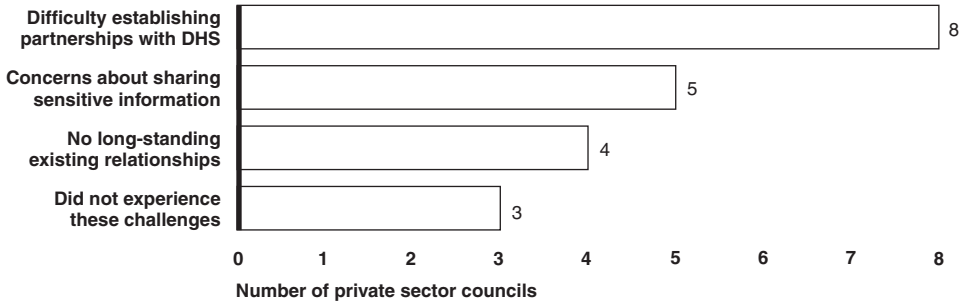
Figure 1: Key Challenges That Affected Establishing Government Councils



Source: GAO analysis.

Note: Values do not add to 17 because council representatives may have indicated more than one challenge.

Figure 2: Key Challenges That Affected Establishing Sector Councils



Source: GAO analysis.

Note: Values do not add to 15 because the 14 council representatives and the rail sector representative may have indicated more than one challenge.

Representatives of Eleven Councils Cited Establishing Partnerships with DHS as a Challenge in Forming Councils

Council representatives with three government and eight sector councils reported that they experienced problems forming their councils due to a number of challenges establishing partnerships with DHS.[13] 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

[13]As noted earlier, DHS serves as the sector-specific agency for ten 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.

acknowledged that its recent reorganization has 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 of the councils. According to this official, DHS has taken a consistent approach to implement the partnership model, and the individual person in a particular staff position does not matter because the DHS implementation guidance is consistent. However, the director acknowledged that continuing staff turnover could affect the eventual success of the government-private sector partnerships because they will be dependent on the actual interactions between the sector-specific agency representatives and the sector council members and the trust they develop. Continuity of government staff is a key ingredient in developing trusted relationships with the private sector.

We and others have similarly reported on DHS's struggles to achieve organizational stability and to provide infrastructure expertise across all sectors in the past as well as in our most recent work on Internet security issues. For example, in May 2005, we reported that DHS faced a number of challenges that impeded its ability to fully address its cybersecurity critical infrastructure protection responsibilities, including achieving organizational stability and establishing effective partnerships with stakeholders.[14] Specifically, we reported that DHS continued to have difficulties in developing partnerships, as called for in federal policy, with other federal agencies, state and local governments, and the private sector. We recommended that DHS engage appropriate stakeholders to prioritize key cybersecurity responsibilities as well as identify performance measures and milestones for fulfilling them. DHS concurred with our recommendation to engage stakeholders in prioritizing its key cybersecurity responsibilities, noting that continued and expanded stakeholder involvement is critical. However, DHS did not agree that the challenges it experienced prevented it from achieving significant results in improving the nation's cybersecurity posture. In addition, DHS did not concur with our recommendations to (1) develop a prioritized list of key activities for addressing the underlying challenges and (2) identify performance measures and milestones for fulfilling its prioritized responsibilities and for performing activities to address its challenges and track organizational progress. Nonetheless, in its strategic plan for

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

cybersecurity, DHS acknowledges that it needs to establish performance measures and milestones and to collect performance data for its key initiatives. More recently, in March 2006, the Council on Foreign Relations, in a study of private sector efforts to protect critical infrastructure, reported that DHS was still struggling with many issues that prevented the full cooperation of the private sector in terms of improving homeland security and protecting critical infrastructure.[15] For example, the council noted that DHS suffered from high management turnover, poor quality management, and a shortage of experienced personnel as factors that contributed to the difficulty in improving relationships with the private sector. Finally, in June 2006, we reported that DHS faced similar challenges that impeded its ability to protect the Internet infrastructure, including organizational and leadership changes at the department.[16]

Representatives for about a Third of Councils Expressed Concerns about Sharing Sensitive Information about Infrastructure Vulnerabilities with the Government and with Other Sector Members

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.[17]

This issue continues to be a longstanding concern and one that contributed to our designating homeland security information sharing as a high-risk issue in January 2005.[18] We reported then that the ability to share

[15]Council on Foreign Relations, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, CSR Number 13 (New York, N.Y.: March 2006).

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

[17]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).

[18]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.

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 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.[19]

More recently, 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.[20] 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 and in September 2006 issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS.

To help address council concerns about sharing sensitive security information, DHS in March 2006 created the Critical Infrastructure

[19]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).

[20]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).

Partnership Advisory Council, open to members of each of the government and sector councils. The purpose of the Advisory Council is to facilitate interactions between government representatives and private sector owners and operators of critical assets. To accomplish this goal, DHS exempted council proceedings from requirements of the Federal Advisory Committee Act. However, it is too soon to determine whether the council has helped facilitate information sharing.

Several Council Representatives Cited a Lack of Prior Working Relationships as a Challenge to Council Formation

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 healthcare sector struggled with creating a sector council that represented the interests of the sector because it is comprised of thousands of entities that are not largely involved with each other in daily activities.[21] 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. Some individual members, such as pharmaceutical companies, do have vigorous critical infrastructure protection programs to address their company's challenges. The official also noted that many other companies work cooperatively to evaluate cybersecurity requirements. However, the official said by and large, such initiatives are unique to specific industries, are not applicable to the entire sector, and are geared to specific business objectives (e.g., prevention of industrial espionage). The official indicated that most sector members have few strong, continuing incentives to collaborate with one another in understanding and resolving critical infrastructure protection-related issues. Despite these reported challenges, the public health and healthcare 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

[21]According to Department of Health and Human Services officials, there are thousands of entities that could be considered stakeholders in the sector. On the public side of the public health and healthcare sector stakeholders include three cabinet level departments (the Department of Health and Human Services, the Department of Defense, and the Department of Veterans Affairs), 57 state and territorial authorities, 3,066 counties, and approximately 10,000 municipalities. On the private side (roughly 92 percent of the total sector), stakeholders are far more numerous. For example, there are over 6,500 hospitals, over 492,000 ambulatory healthcare facilities, and nearly 70,000 nursing and residential care facilities.

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 comprising 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. The council has established eight subcouncils to allow the disparate members to organize in a meaningful way. Because approximately 85 percent of the nation's critical infrastructure is owned by the private sector, developing trusted partnerships between the federal government and the private sector across all sectors is critical to ensure the protection of these assets, as we reported in 2001 and in a number of subsequent reports on critical infrastructure protection issues.

Councils Delayed Their Work on Sector-Specific Plans until the NIPP Was Issued but Despite Challenges, Expect to Complete Plans by the End of December 2006

Each of the 17 sectors is preparing sector-specific plans. Sector-specific agencies anticipate that all plans will be finalized by the end of December 2006, as required by the NIPP, but some sectors were farther along than others as of August 2006. 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 lack 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 Believe They Will Complete Plans on Time

Sector-specific agency representatives believe they will meet the deadline to complete their plans by December 2006.[22] DHS 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. Nevertheless, as of August 2006, some sectors reported being further along in developing a plan than others, and some private council representatives said collaboration between the private council and the government council on the plans had yet to take place. For example, representatives of the chemical and nuclear sectors anticipated completing their plans before the December deadline. However, while TSA officials reported that they had drafted an overall plan, they had only begun drafting plans for each transportation mode such as aviation, rail, and ports, as of August 2006. Additionally, the overall plan had yet to be shared with the private sector at the time of our review. Moreover, the commercial facilities sector-specific agency representative said that as of May 2006, the agency had only developed a plan outline because it was still conducting outreach with the sector council and other relevant government councils. Nevertheless, the sector co-chair said the sector should be able to meet the December 2006 deadline.

The NIPP 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.[23] For example, the Department of Agriculture and the Food and Drug Administration are initiating a draft agriculture and food plan and plan to

[22]DHS has delegated plan preparation responsibilities among several of its component agencies for the 10 sectors for which DHS is the designated sector-specific agency. Specifically, DHS's Office of Infrastructure Protection is the sector-specific agency for the chemical; commercial facilities; dams; emergency services; and commercial nuclear reactors, materials, and waster sectors. The Office of Cyber Security and Telecommunications is the sector-specific agency for the information technology and telecommunications sectors. The Transportation Security Administration (TSA) is the sector-specific agency for the postal and shipping sector and jointly shares responsibility for transportation systems with the U.S. Coast Guard. The Federal Protective Service is responsible for the government facilities sector.

[23]Two sectors, government facilities and national monuments and icons, do not have private sector councils.

provide it to a working group of government and sector council representatives to add relevant information and comments, while representatives of the energy sector council are working with the Department of Energy to draft the energy plan. Despite the consistent belief among the sectors that they will be able to provide their plans to DHS by the December 2006 deadline, the extent to which some of the sector-specific agencies that are responsible for the less developed and organized sectors are going to be able to achieve the required collaboration is uncertain since effective relationships within the sectors and with federal agencies had yet to be established, which is a crucial step.

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

Representatives from both sector-specific agencies and sector councils identified a number of factors that have helped in the development of their plans. The most common factors included having (1) pre-existing plans, (2) pre-existing relationships between the government and the private sector, and (3) assistance from DHS officials and contractors. 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 ("Y2K") 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. Likewise, HHS and U.S. Department of Agriculture representatives said that the agriculture and food plan will follow and document infrastructure protection practices that the sector was already doing as a result of Homeland Security Presidential Directive 9 (HSPD-9)—which established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies—and will be based on a previous plan developed in 2004 in response to the directive. 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. Representatives from the Transportation Security Administration (TSA) and the banking and finance government council also said that previous regulatory relationships with their sectors helped with plan development. The TSA official said that the flow of information and coordination between the federal government and the transportation industry occurred continually and that these existing networks would also assist in plan development. Sectors with operating ISACs—such as the telecommunications and information technology sectors—found them to have assisted in developing sector-specific plans because of their longer involvement in public-private information sharing. 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. In addition, according to officials on the telecommunications sector council's steering committee, communications companies, electric power suppliers, and information technology providers have a history of working together to ensure the continuity of services during potentially disrupting events. This history facilitated cooperation and coordination in developing the sector-specific plans.

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. In addition to the contractor assistance identified above, DHS entered into the following contract to provide support for the development of the NIPP and the sector-specific plans:

- DHS contracted with ICF International, a professional services consulting firm, in January 2004. Under this contract, ICF International was to support the development of the guidance for the sector-specific plans, conduct technical assistance sessions for sector-specific agencies to facilitate plan development, and provide subject matter experts to each of the 17 sectors to support drafting and review of each sector's plan. According to DHS, ICF International was provided $11.2 million for work performed from January 2004 through December 2006.

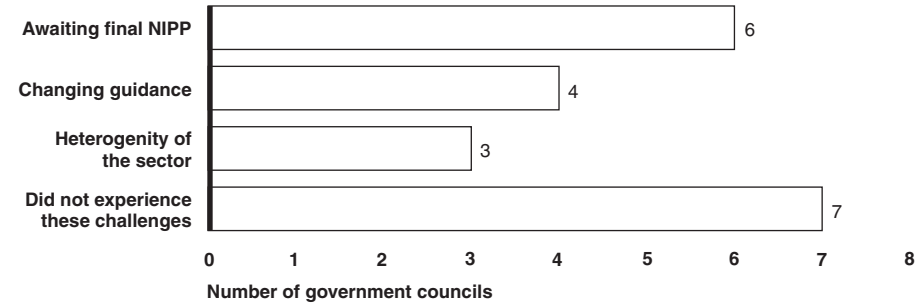
Representatives from the national monuments and icons and the government facilities sectors said that DHS officials have been accessible

and responsive to questions regarding plan guidance. In addition, five sector representatives cited the help provided through DHS's contract with the George Mason University's Critical Infrastructure Protection program as being useful in understanding the plan guidance and in facilitating sector communication. These and other sector representatives said that the DHS-provided contractor assistance also helped in the development of their plans. By having access to these contractors, sectors were able to access additional support when needed for plan development activities 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 Lack of a Final NIPP, Changing Guidance, and Other Challenges Impeded Progress on Some Sector-Specific Plans

The most common key challenges sector representatives reported as having contributed to delays in the development of their plans included (1) the lack of a final NIPP, (2) changing DHS guidance, and (3) the diverse makeup of sector membership. Representatives from seven government councils and six private councils did not report any major challenges to plan development. Figures 3 and 4 summarize the key challenges in developing plans cited by council representatives.

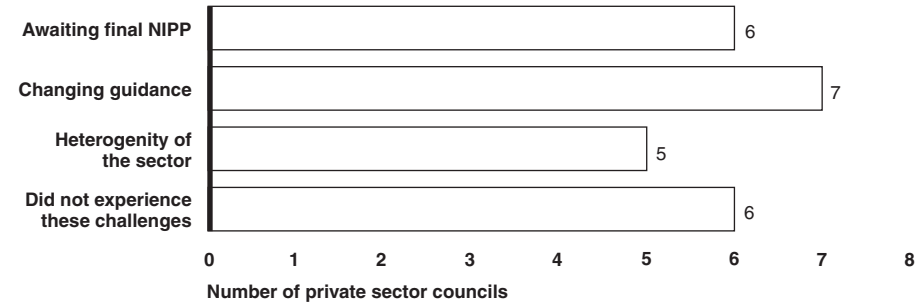
Figure 3: Key Challenges to Developing Sector-Specific Plans, according to Government Council Representatives



Source: GAO analysis.

Note: Values do not add to 17 because council representatives may have indicated more than one challenge.

Figure 4: Key Challenges to Developing Sector-Specific Plans, according to Sector Council Representatives



Source: GAO analysis.

Note: Values do not add to 15 because the 14 council representatives and the rail sector representative may have indicated more than one challenge.

Representatives from six government councils and six sector councils said that the lack of a final NIPP contributed to delays in developing their sector plans. Furthermore, representatives with three sectors specifically stated that they suspended revisions to their sector plans primarily because they wanted to be sure the plans followed the requirements in the final NIPP and to minimize revisions. The sector-specific agencies are required to complete their plans and submit them to DHS 180 days from the final issuance date of the NIPP. Since DHS issued the final NIPP in June 2006, the agencies have until the end of December 2006 to submit their plans. According to DHS, sectors had begun drafting their sector-specific plans following the issuance of initial sector-specific plan guidance in April 2004. After DHS issued the interim NIPP in February

2005, it continued to refine the NIPP based on stakeholder comments and also issued revised sector-specific plan guidance. For example, DHS revised its 2004 plan guidance 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 that required the plans to have a new chapter describing 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.

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 five sectors also reported that DHS incorporated changes to address their concerns. For example, representatives from the information technology, public health, energy, telecommunications, and transportation systems sectors, among others, had commented that the NIPP should emphasize resiliency rather than protection. 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 this concept of resiliency into the final NIPP to address these concerns.

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, as noted earlier, the commercial facilities sector is comprised 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.

Concluding Observations

Critical infrastructure protection is vital to our national security, economic vitality and public health. Significant damage to critical infrastructure and key resources could disrupt the functioning of business and government alike, underscoring the need for the private and public sectors to take a coordinated approach to critical infrastructure protection. While DHS is to be commended for its efforts to incorporate private sector comments into the final NIPP, the 18-month delay in issuing that document and changing DHS planning guidance have slowed down the progress of some sectors in developing specific plans to protect sectors. As a result, some less mature sectors were still in the outline phase of developing their sector-specific plans at the time of our review, leaving much to do and not a lot of time left to do it before the December deadline. In addition, some private council representatives said collaboration between the private council and the government council on the plans, which is required by the NIPP, had yet to take place. Not only is this collaboration required by the NIPP, but also the ability of the private sector to achieve the goals of HSPD-7 and the National Strategy for Homeland Security depends on it. The extent to which some of the sector-specific agencies that are responsible for the less developed councils and plans are going to be able to achieve this collaboration is uncertain since neither had yet established effective relationships, a crucial step. In addition, both the NIPP and the sector plans only represent a first step toward ensuring sufficient protection of critical infrastructure. The NIPP lays out guidance for critical infrastructure protection planning and risk assessments, yet the sector plans must only demonstrate how the sectors will identify their critical assets, plan for infrastructure protection, and assess risk across their infrastructure base, not identify critical assets and assess risk levels. Conducting these identifications and assessments will be the next step under the NIPP guidelines.

The inability to share information critical to homeland security and infrastructure protection continues to pose a significant risk to the nation. This report, as well as our past work, demonstrates that many private

sector partners do not trust the government enough yet to share information on their security vulnerabilities. DHS's creation of the Critical Infrastructure Partnership Advisory Council in March 2006 may help alleviate private sector concerns about the sharing of sensitive security information, but it is too soon to determine whether the council has helped facilitate information sharing. Similarly, developing successful working relationships continues to be an important issue for DHS. Our previous work, dating back to 2001, shows that the establishment of trusted relationships is vital to the success of information sharing and critical infrastructure protection efforts. Given the long-term relationships that are necessary for the successful implementation of the NIPP, factors that impact these relationships, such as continuing staff turnover, could affect the eventual success of the government-private sector partnerships. Because our findings in this report echo many of those in our previous reports and are covered by previous recommendations to DHS that have yet to be fully implemented, we are not making any new recommendations at this time. Continued monitoring will determine whether further recommendations are warranted.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies of this report to appropriate departments and interested congressional committees. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or at larencee@gao.gov. Key contributors to this report are listed in appendix IV.

Eileen R. Larence
Director, Homeland Security and Justice Issues

Appendix I: Key Federal Initiatives in Developing Critical Infrastructure Protection Policy, 1996 to Present

Policy action	Date	Key elements
Executive Order 13010	July 1996	Established the President's Commission on Critical Infrastructure Protection to study the nation's vulnerabilities to both cyber and physical threats. Identified the need for the government and the private sector to work together to establish a strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.
Presidential Decision Directive 63	May 1998	Established CIP as a national goal and presented a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. Designated government agencies to coordinate and support CIP efforts. Identified lead federal agencies to work with coordinators in eight infrastructure sectors and five special functions. Encouraged the development of information-sharing and analysis centers; Required every federal department and agency to be responsible for protecting its own critical infrastructures, including both cyber-based and physical assets. Superseded by HSPD-7 (see details on HSPD-7 below).
National Plan for Information Systems Protection[a]	Jan. 2000	Provided a vision and framework for the federal government to prevent, detect, and respond to attacks on the nation's critical cyber-based infrastructure and to reduce existing vulnerabilities via federal computer security and information technology requirements.
Executive Order 13228	Oct. 2001	Established the Office of Homeland Security, within the Executive Office of the President, to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. Established the Homeland Security Council to advise and assist the President with all aspects of homeland security and to ensure the coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies.
Executive Order 13231	Oct. 2001	Established the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures and to recommend policies and coordinating programs for protecting CIP-related information systems.
National Strategy for Homeland Security[b]	July 2002	Identified the protection of critical infrastructures and key assets as a critical mission area for homeland security. Expanded the number of critical infrastructures from the 8 (identified in Presidential Decision Directive 63) to 13 and identified lead federal agencies for each. Specified 8 major initiatives for CIP, one of which specifically calls for the development of the National Infrastructure Protection Plan.

Policy action	Date	Key elements
Homeland Security Act of 2002[c]	Nov. 2002	Created the Department of Homeland Security and assigned it the following CIP responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other entities; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets[d]	Feb. 2003	Provided a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. Built on Presidential Decision Directive 63 with its sector-based approach and called for expanding the capabilities of information sharing and analysis centers. Outlined three key objectives: (1) identifying and assuring the protection of the most critical assets, systems, and functions; (2) assuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to assure the protection of other potential targets.
Executive Order 13286	Feb. 2003	Amended Executive Order 13231 but generally maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures. Designated the National Infrastructure Advisory Council to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy through the Secretary of Homeland Security.
Homeland Security Presidential Directive 7	Dec. 2003	Superseded Presidential Decision Directive 63 and established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. Defined roles and responsibilities for the Department of Homeland Security and sector-specific agencies to work with sectors to coordinate CIP activities. Established a CIP Policy Coordinating Committee to advise the Homeland Security Council on interagency CIP issues.

Source: GAO analysis of documents listed above.

[a]The White House, Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue (Washington, D.C.: January 2000).

[b]The White House, Office of Homeland Security, National Strategy for Homeland Security.

[c]Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[d]The White House, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

Appendix II: Government Sector Council Membership, by Sector as of August 2006

Sector	Government council members
Agriculture and food	Association of State and Territorial Health Officials
	Intertribal Agriculture Council
	National Assembly of State Chief Livestock Health Officials
	National Association of County and City Health Officials
	National Association of State Departments of Agriculture
	US Dept. of Agriculture
	US Dept. of Defense
	US Dept. of Health and Human Services
	US Dept. of Homeland Security
	US Environmental Protection Agency
	Ex Officio Members:
	Association of Food and Drug Officials
	US Dept. of Commerce
	US Dept. of Justice
	US Dept. of the Interior
Banking and finance	Commodity Futures Trading Commission
	Conference of State Bank Supervisors
	Farm Credit Administration
	Federal Deposit Insurance Corporation
	Federal Housing Finance Board
	Federal Reserve Bank of New York
	Federal Reserve Board
	National Association of Insurance Commissioners
	National Association of State Credit Union Supervisors
	National Credit Union Administration
	North American Securities Administration Association
	Office of Federal Housing Enterprise Oversight
	Office of the Comptroller of the Currency
	Office of Thrift Supervision
	Securities and Exchange Commission
	Securities Investor Protection Corporation
	US Dept. of Treasury

Sector	Government council members
Chemical	US Dept. of Commerce
	Bureau of Industry and Security
	US Dept. of Homeland Security
	Preparedness Directorate, National Cyber Security Division
	Preparedness Directorate, Office of Infrastructure Protection
	Science and Technology Directorate
	Transportation Security Administration
	US Coast Guard
	US Dept. of Justice
	Bureau of Alcohol, Tobacco, Firearms and Explosives
	Federal Bureau of Investigation
	US Dept. of Transportation
	Federal Railroad Administration
	Federal Motor Carrier Safety Administration
	Pipeline and Hazardous Materials Safety Administration
	US Environmental Protection Agency
	Office of Emergency Management
	Water Security Division
Commercial facilities	National Endowment for the Arts
	US Dept. of Commerce
	US Dept. of Education
	US Dept. of Homeland Security
	Immigration and Customs Enforcement's Federal Protective Service
	Office of Infrastructure Protection, Risk Management Division
	Private Sector Office
	US Dept. of Housing and Urban Development
	US Dept. of the Interior
	US Environmental Protection Agency
	US General Services Administration
	US Secret Service
	Ex Officio Members:
	US Dept. of Health and Human Services
	US Dept. of Justice

Sector	Government council members
Commercial nuclear reactors, materials, and waste	Nuclear Regulatory Commission
	US Dept. of Defense
	US Dept. of Energy
	US Dept. of Homeland Security
	Office of Infrastructure Protection, Chemical & Nuclear Preparedness and Protection Division
	Science and Technology Directorate
	US Coast Guard
	US Dept. of Justice
	Federal Bureau of Investigation
	US Environmental Protection Agency
Dams	Federal Energy Regulatory Commission
	State of California, Department of Water Resources
	State of New Jersey, Department of Environmental Protection
	State of Ohio, Department of Natural Resources
	State of Virginia, Department of Conservation and Recreation
	State of Washington, Department of Ecology
	Tennessee Valley Authority
	US Dept. of Agriculture, Natural Resources Conservation Service
	US Dept. of Defense, US Army Corps of Engineers
	US Dept. of Homeland Security
	Office of Infrastructure Protection, Risk Management Division
	US Dept. of Labor, Mine Safety and Health Administration
	US Dept. of State, International Boundary and Water Commission
	US Dept. of the Interior, Bureau of Reclamation
	US Environmental Protection Agency

Sector	Government council members
Defense industrial base	US Dept. of Defense
	Assistant Secretary of Defense (Homeland Defense)
	Director, Defense Critical Infrastructure Program
	Deputy Under Secretary of Defense (Industrial Policy)
	Director, Defense Procurement & Acquisition Policy
	Deputy Under Secretary of Defense (International Technology Security)
	Director, Technology Assessments
	Director, Defense Contract Management Agency
	Director, Industrial Analysis Center
	Deputy Under Secretary of Defense (Personnel & Readiness)
	Director, Readiness Programming and Assessment
	Deputy Chief Information Officer
	Office of the DASD for Information Management and Technology
	Director, Architecture & Interoperability
	Director, National Guard Bureau
	Director, NGB-J3
	US Dept. of Homeland Security
	Office of the Assistant Secretary of Homeland Security (Infrastructure Protection)
	US Dept. of Treasury
	Committee on Foreign Investment in the United States
	Office of Critical Infrastructure Protection & Compliance Policy
	US Dept. of Justice
	Federal Bureau of Investigation
	US Dept. of Commerce
	Office of Strategic Industries and Economic Security, Bureau of Industry and Security

Sector	Government council members
Drinking water and water treatment systems	Association of State and Interstate Water Pollution Control Administrators
	Association of State Drinking Water Administrators
	US Army Corps of Engineers
	US Dept. of Agriculture
	Natural Resources Conservation Service
	US Dept. of Defense
	US Dept. of Health and Human Services
	US Dept. of Homeland Security
	Information Analysis and Infrastructure Protection/Information Coordination Division
	US Dept. of State
	US Dept. of the Interior
	Bureau of Reclamation
	US Environmental Protection Agency
Emergency services	American Red Cross
	US Dept. of Health and Human Services
	US Dept. of Homeland Security
	Border & Transportation Security
	Office of Infrastructure Protection, Chemical & Nuclear Preparedness and Protection Division
	Federal Emergency Management Agency
	Fire Administration
	Immigration Customs & Enforcement
	Office of Infrastructure Protection, Infrastructure Partnerships Division
	Infrastructure Programs Office
	Office of Grants & Training
	Office of Public Health Emergency Preparedness
	Science and Technology Directorate
	Office of State and Local Government Coordination
	Office of Infrastructure Protection, Risk Management Division
	US Coast Guard
	US Dept. of Transportation
	National Highway Traffic Safety Administration
	US Secret Service

Sector	Government council members
Energy	Federal Energy Regulatory Commission
	National Association of Regulatory Utility Commissioners
	National Association of State Energy Officials
	US Dept. of Agriculture
	Rural Utility Service
	US Dept. of Defense
	US Army Corps of Engineers
	US Dept. of Energy
	Office of Infrastructure Security and Energy Restoration
	Western Area Power Administration
	US Dept. of Homeland Security
	Infrastructure Partnerships Division
	Office of Infrastructure Protection, Risk Management Division
	Transportation Security Administration
	US Coast Guard
	US Dept. of the Interior
	Minerals Management Service
	US Dept. of State
	International Boundary and Water Commission
	US Dept. of Transportation
	Research & Special Programs Administration
	Maritime Administration
	US Environmental Protection Agency
Government facilities	US Capitol Police Intelligence Section
	US Department of Agriculture
	Office of Facility Security
	US Department of Commerce
	Anti-Terrorism Division
	US Department of Defense
	Office of the Assistant Secretary of Defense, Homeland Defense,
	Critical Infrastructure Protection
	Office of Installations Requirements and Management
	Air National Guard
	US Department of Education
	US Department of Energy
	Office of the Deputy Under Secretary for Counterterrorism
	US Department of Health and Human Services
	Departmentwide Security

Sector	Government council members
	US Department of Homeland Security
	Preparedness Directorate
	Office of Infrastructure Protection
	Risk Management Division
	Infrastructure Partnerships Division
	National Cyber Security Division
	Science and Technology Directorate
	Federal Emergency Management Administration
	US Coast Guard
	US Secret Service
	Customs and Border Protection
	Immigration and Customs Enforcement
	US Department of Justice
	US Marshals Service, Judicial Security Division, Judicial Security Systems
	FBI, Special Advisor to the DHS G&T, Office of Law Enforcement Coordination
	US Department of Labor
	Director of Security
	US Department of State
	Bureau of Resources Management, Intelligence, Resources, and Planning, and Critical Infrastructure Protection
	US Department of the Interior
	Law Enforcement and Security
	National Park Service
	US Department of the Treasury
	Critical Infrastructure Physical Security, Cyber Security
	US Department of Transportation
	Federal Aviation Administration, Security and Hazardous Materials, Internal Security Division
	US Department of Veterans Affairs
	Office of Security and Law Enforcement
	US Postal Inspection Service
	Administrative Offices of the US Courts-Court Security Office
	Architect of the Capital
	Environmental Protection Agency
	Federal Facilities Council
	General Services Administration
	Interagency Security Committee
	National Aeronautical and Space Administration

Sector	Government council members
	National Archives and Records Administration
	National Center for State Courts
	Office of Personnel Management
	Social Security Administration
Information technology	Director of National Intelligence
	Metropolitan Information Exchange
	National Association of State Chief Information Officers
	National Institute of Standards and Technology
	Office of Management and Budget
	US Dept. of Commerce
	US Dept. of Defense
	US Dept. of Homeland Security
	US Dept. of Justice
	US Dept. of State
	US Dept. of the Treasury
National monuments and icons	National Archives and Records Administration
	Smithsonian Institute
	US Capitol Police
	US Dept. of Defense
	US Dept. of Homeland Security
	Immigration and Customs Enforcement, Office of Federal Protective Service
	US Dept. of the Interior
	National Park Service
	US Park Police
	US Secret Service
Postal and shipping	US Dept. of Defense
	US Dept. of Health and Human Services
	Office of Public Health Emergency Preparedness
	Food and Drug Administration
	US Dept. of Homeland Security
	Customs and Border Protection
	Preparedness Directorate
	Science and Technology Directorate
	US Dept. of Justice

Sector	Government council members
Public health and healthcare	American Red Cross
	Association of Public Health Laboratories
	Association of State and Territorial Health Officials
	District of Columbia Department of Health
	Federal Emergency Management Administration
	General Services Administration
	Indian Health Service Tribal Council
	National Association of County and City Health Officials
	US Dept. of Agriculture
	US Dept. of Defense
	US Dept. of Health and Human Services
	US Dept. of Homeland Security
	US Dept. of Transportation
	US Dept. of Veterans Affairs
	US Environmental Protection Agency
	US Postal Service
	White House Office of Science and Technology Policy
Telecommunications	Federal Communications Commission
	US Dept. of Commerce
	National Telecommunications and Information Administration
	US Dept. of Defense
	Office of the Secretary of Defense, Networks and Information Integration
	US Dept. of Homeland Security
	National Communication System
	Preparedness Directorate, National Cyber Security Division
	US Dept. of Justice
	US General Services Administration
Transportation systems	US Dept. of Defense
	US Dept. of Energy
	US Dept. of Homeland Security
	Infrastructure Partnerships Division
	Transportation Security Administration
	US Coast Guard
	US Dept. of Transportation

Source: Government council representatives and DHS.

Appendix III: Sector Council Membership, by Sector as of August 2006

Sector	Sector council members
Agriculture and food	Agricultural Retailers Association
	American Farm Bureau Federation
	CF Industries, Inc.
	CropLife America
	Food Marketing Institute
	Food Products Association
	International Association of Refrigerated Warehouses
	International Dairy Foods Association
	International Food Service Distributors Association
	International In-flight Food Service Association
	International Warehouse Logistics Association
	McCormick & Company, Inc.
	National Association of Convenience Stores
	National Cattlemen's Beef Association
	National Corn Growers Association
	National Food Service Security Council
	National Milk Producers Federation
	National Pork Producers Association
	National Restaurant Association
	National Retail Federation
	TD Enterprises
	United Fresh Fruit & Vegetable Association

Sector	Sector council members
Banking and finance	American Bankers Association
	American Council of Life Insurers
	American Insurance Association
	American Society for Industrial Security International
	America's Community Bankers
	BAI
	BITS/The Financial Services Roundtable
	Chicago Mercantile Exchange
	ChicagoFIRST, LLC
	CLS Group
	Consumer Bankers Association
	Credit Union National Association
	Fannie Mae
	Financial Information Forum
	Futures Industry Association
	Independent Community Bankers of America
	Investment Company Institute
	Managed Funds Association
	NACHA—The Electronic Payments Association
	National Association of Federal Credit Unions
	National Association of Securities Dealers
	New York Board of Trade
	Securities Industry Association
	Securities Industry Automation Corporation
	The Bond Market Association
	The Clearing House
	The Depository Trust & Clearing Corporation
	The NASDAQ Stock Market, Inc.
	The Options Clearing Corporation
	VISA USA Inc

Sector	Sector council members
Chemical	American Chemistry Council
	American Forest & Paper Association
	Agriculture Retailers Association
	Chemical Producers & Distributors Association
	Chlorine Chemistry Council
	Compressed Gas Association
	Crop Life America
	Independent Liquid Terminals Association
	Dupont
	Institute of Makers of Explosives
	International Institute of Ammonia Refrigeration
	National Association of Chemical Distributors
	National Paint & Coatings Association
	National Petrochemical & Refiners Association
	Synthetic Organic Chemical Manufacturers Association
	The Adhesive and Sealant Council
	The Chlorine Institute
	The Fertilizer Institute
	The Society of the Plastics Industry, Inc.
Commercial facilities	The council is comprised of 30 individuals who represent the eight subcouncils. These subcouncils currently incorporate over 200 members. Coordination across subcouncils happens at the council level. Subcouncils are: Public Assembly Facilities; Sports Leagues; Resorts; Lodging; Outdoor Event Facilities; Entertainment and Media; Real Estate; and Retail.
Commercial nuclear reactors, materials, and waste	Arizona Public Service Company
	Constellation Energy Generation Group
	Dominion Energy
	Dominion Generation
	Entergy Operations
	Excelon Generation Company, LLC
	General Electric Energy Nuclear Energy
	National Institute of Standards and Technology
	Nuclear Energy Institute
	Southern Nuclear Company
	USEC Inc

Sector	Sector council members
Dams	Allegheny Energy
	Ameren Services Company
	American Electric Power
	Association of State Dam Safety Officials
	AVISTA Utilities
	Canadian Dam Association
	Chelan County
	CMS Energy
	Dominion Resources
	Duke Energy Corporation
	Exelon Corporation
	National Hydropower Association
	National Mining Association
	New York City, Department of Environmental Protection
	New York Power Authority
	Pacific Gas & Electric Company
	PPL Corporation
	Scana Corporation
	South Carolina Public Service Authority
	Southern California Edison
	Southern Company Generation
	TransCanada
	United States Society of Dams
	Xcel Energy Corporation
Defense industrial base	Aerospace Industries Association
	American Society for Industrial Security
	Armed Forces Communications and Electronics Association
	Contractor Secret Asset Programs Security Working Group
	Industrial Security Working Group
	National Classification Management Society
	National Defense Industrial Association

Sector	Sector council members
Drinking water and water treatment systems	The council consists of two owner/operator representatives, along with one non-voting association staff member, from each of the eight water associations.
	Alexandria Sanitation Authority
	American Water
	American Water Works Association
	American Water Works Association Research Foundation
	Association of Metropolitan Water Agencies
	Bean Blossom Patricksburg Water Corporation
	Boston Water and Sewer Commission
	Breezy Hill Water and Sewer Company
	City of Portland Bureau of Environmental Services
	City of Richmond, Department of Public Utilities
	Columbus Water Works
	East Bay Municipal Utility District
	Fairfax Water
	Greenville Water System
	Los Angeles Department of Water and Power
	Manchester Water Works
	National Association of Clean Water Agencies
	National Association of Water Companies
	National Rural Water Association
	New York City Department of Environmental Protection
	Pima County Wastewater Management Department
	United Water
	Water Environment Federation
	Water Environment Research Foundation
Emergency services	International Association of Chiefs of Police
	International Association of Emergency Managers
	International Association of Fire Chiefs
	National Association of State EMS Officials
	National Emergency Management Association
	National Sheriff's Association
Energy	American Gas Association
	American Petroleum Institute
	American Public Gas Association
	Anadarko Canada Corp.
	Anadarko Petroleum Corporation
	Arizona Public Service Company
	Association of Oil Pipe Lines

Sector	Sector council members
	BP
	Canadian Association of Petroleum Producers
	Chevron Corporation
	ConocoPhillips
	Domestic Petroleum Council
	Dominion Resources Inc.
	Edison Chouest Offshore, LLC
	El Paso Corp.
	Energy ISAC
	Exelon Corporation
	ExxonMobil
	Gas Processors Association
	Independent Electricity System Operator, Ontario Canada
	Independent Liquid Terminals Association
	Independent Petroleum Association of America
	International Association of Drilling Contractors
	Interstate Natural Gas Association of America
	Leffler Energy
	Marathon Petroleum Company, LLC
	National Association of Convenience Stores
	National Ocean Industries Association
	National Petrochemical & Refiners Association
	National Propane Gas Association
	National Rural Electric Cooperative Association
	New York Independent System Operator
	Newfoundland Ocean Industries Association
	NiSource, Inc.
	North American Electric Reliability Council
	Offshore Marine Service Association
	Offshore Operators Committee
	Petroleum Marketers Association of America
	Reliability First Corporation
	Rowan Companies, Inc.
	Shell Oil Company
	Shipley Stores, LLC
	Society of Independent Gasoline Marketers of America
	Southern Company Services, Inc.
	U.S. Oil & Gas Association

Sector	Sector council members
	Valero Energy Corporation
	Western States Petroleum Association
Government facilities	Not applicable[a]
Information technology	Bell Security Solutions Inc.
	BellSouth Corporation
	Center for Internet Security
	Cisco Systems, Inc.
	Citadel Security Software, Inc.
	Computer and Communications Industry Association
	CA, Inc.
	Computer Sciences Corporation
	Computing Technology Industry Association
	Cyber Security Industry Alliance
	Electronic Industries Alliance
	Entrust, Inc.
	EWA Information & Infrastructure Technologies, Inc.
	IBM Corporation
	Information Systems Security Association
	Information Technology - Information Sharing & Analysis Center
	Information Technology Association of America
	Intel Corporation
	International Security, Trust, and Privacy Alliance
	International Systems Security Engineering Association
	Internet Security Alliance
	Internet Security Systems
	KMPG LLC
	Lockheed Martin
	McAfee, Inc.
	Microsoft Corporation
	NTT America
	R&H Security Consulting LLC
	Seagate Technology
	Symantec Corporation
	U.S. Internet Service Provider Association
	Unisys Corporation
	VeriSign
	Verizon
National monuments and icons	Not applicable[a]

Sector	Sector council members
Postal and shipping	DHL
	FedEx Corp.
	United Parcel Service
	US Postal Service
Public health and healthcare	AABB (formerly the American Association of Blood Banks)
	Advanced Medical Technology Association (AdvaMed)
	Aiken Regional Medical Centers
	Air Force Medical Support Agency, Medical Logistics Division
	American Association of Colleges of Nursing
	American Association of Occupational Health Nurses, Inc.
	American College of Occupational & Environmental Medicine
	American Hospital Association
	American Industrial Hygiene Association
	American Medical Association
	American Medical Depot
	American Nurses Association
	American Red Cross
	Association for Healthcare Resources & Materials Management
	Association of State and Territorial Directors of Nursing
	Association of State and Territorial Health Officials
	BASF Corporation
	Baylor Healthcare System
	Biotechnology Industry Organization
	BlueCross BlueShield Association
	California Hospital Association
	Cedars-Sinai Hospital
	Chamber of Commerce Manhattan Beach
	Childrens Hospital Los Angeles
	Columbia University School of Nursing
	Concentra, Inc.
	Cremation Association of North America
	Cumberland Plateau Health District, Buchanan, Dickenson, Russell and Tazewell County Health Departments
	Dartmouth Hitchcock Medical Center
	DST Output
	Duke University Medical Center
	Eli Lilly
	ER One Institutes for Innovation in Medicine/Institute for Medical Informatics, Washington Hospital Center

Sector	Sector council members
	Exponent, Inc.
	ExxonMobil
	Florida Department of Health/Office of Public Health Nursing
	Florida Hospital Association
	Greater NY [City] Hospital Association
	Health Industry Distributors Association
	Health Information and Management Systems Society
	Healthways, Inc.
	HemoSense, Inc.
	Henry Schein, Inc
	Hill-Rom
	Honeywell International
	Hospital Association of Southern California
	ICFA - International Cemetery & Funeral Association
	ICTM/Intercet, Ltd.
	INOVA Health System
	International Chemical Workers Union Council/United Food and Commercial Workers
	International Coalition for Mass Casualty Education
	James B. Haggin Memorial Hospital
	John Deere Harvester Works
	Johns Hopkins University/Johns Hopkins Health System
	Johnson & Johnson Health Care Systems
	Joint Council on Accreditation of Healthcare Organizations
	Kaiser Permanente/TPMG Executive Offices
	Kent & O'Connor
	LA Biomedical Research
	LabCorp
	Los Angeles Chamber of Commerce
	McKesson
	MedStar Health, Washington National Medical Center
	Memorial Sloan Kettering Cancer Center
	Metropolitan Chicago Hospital Council
	Nassau County, NY Office of Emergency Management
	National Association of County and City Health Officials
	National Council of State Boards of Nursing
	National Defense University/Information Resources Management College
	National Funeral Directors and Mortuary Association
	National Funeral Directors Association

Sector	Sector council members
	Nevada Hospital Association
	Occidental Chemical Corporation
	Oschner Foundation Hospital
	Owens & Minor
	Pfizer
	Pharmaceutical Research and Manufacturers of America
	PSE&G (Exelon Electric & Gas)
	Quest Diagnostics
	Samaritan Health Services
	The George Washington University Medical Center
	The Regence Group
	The Regional Medical Center, Cook and Associates
	United States Army Medical Research Institute of Chemical Defense
	University of Illinois at Chicago, School of Public Health
	University of North Carolina, School of Public Health
	University of Pittsburgh Medical Center
	Vanderbilt School of Nursing
	Vanderbilt University
	Vanderbilt University Medical Center
	VerdaSee Solutions, Inc.

Sector	Sector council members
Telecommunications	Americom
	AT&T
	BellSouth
	Boeing
	Cellular Telecommunications & Internet Association
	Cincinnati Bell
	Cingular Wireless
	Cisco Systems
	Computer Sciences Corporation
	Internet Security Alliance
	Intrado
	Level 3 Communications
	Lucent Technologies
	McLeodUSA
	Qwest Communications
	Rural Cellular Association
	Satellite Industry Association
	Savvis
	Sprint-Nextel
	Telecommunications Industry Association
	U.S. Internet Service Provider Association
	United Telecom Council
	USTelecom Association
	VeriSign
	Verizon
Transportation systems	Council not yet developed

Source: Sector council representatives and DHS.

[a]There is no private sector component to this sector.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Eileen R. Larence (202) 512-8777

Staff Acknowledgments

In addition to those named above, R.E. Canjar, William Carrigg, Michael Gilmore, Thomas Lombardi, Linda Miller, Dave Powner, Susan H. Quinlan, Nik Rapelje, Deena D. Richart, and E. Jerry Seigler made key contributions to this report.

Related GAO Products

Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity. GAO-06-1087T. Washington, D.C.: Sept. 13, 2006.

Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan. GAO-06-672. Washington, D.C.: June 16, 2006.

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.

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.

Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed. GAO-06-150. Washington, D.C.: January 27, 2006.

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-05-851. Washington, D.C.: September 9, 2005.

Critical Infrastructure Protection: Challenges in Addressing Cybersecurity. GAO-05-827T. Washington, D.C.: July 19, 2005.

Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism. GAO-05-790. Washington, D.C.: June 24, 2005.

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

Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges. GAO-05-327. Washington, D.C.: March 28, 2005.

High-Risk Series: An Update. GAO-05-207. Washington, D.C.: January 1, 2005.

Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices. GAO-05-49. Washington, D.C.: November 30, 2004.

Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters. GAO-04-984. Washington, D.C.: September 27, 2004.

Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities. GAO-04-1023R. Washington, D.C.: August 10, 2004.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

Technology Assessment: Cybersecurity for Critical Infrastructure Protection. GAO-04-321. Washington, D.C.: May 28, 2004.

Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors. GAO-04-699T. Washington, D.C.: April 21, 2004.

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. GAO-04-628T. Washington, D.C.: March 30, 2004.

Water Infrastructure: Comprehensive Asset Management Has Potential to Help Utilities Better Identify Needs and Plan Future Investments. GAO-04-461. Washington, D.C.: March 19, 2004.

Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. GAO-04-354. Washington, D.C.: March 15, 2004.

Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies. GAO-04-157. Washington, D.C.: December 15, 2003.

Posthearing Questions from the September 17, 2003, Hearing on Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness". GAO-04-300R. Washington, D.C.: December 8, 2003.

Critical Infrastructure Protection: Challenges in Securing Control Systems. GAO-04-140T. Washington, D.C.: October 1, 2003.

Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments. GAO-03-502. Washington, D.C.: May 1, 2003.

Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. GAO-03-233. Washington, D.C.: February 28, 2003.

Potential Terrorist Attacks: More Actions Needed to Better Prepare Critical Financial Markets. GAO-03-468T. Washington, D.C.: February 12, 2003.

Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats. GAO-03-173. Washington, D.C.: January 30, 2003.

Critical Infrastructure Protection: Significant Challenges Need to Be Addressed. GAO-02-961T. Washington, D.C.: July 24, 2002.

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems. GAO-02-474. Washington, D.C.: July 15, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection. GAO-02-24. Washington, D.C.: October 15, 2001.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

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