United States Government Accountability Office

GAO

Testimony before the Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate

For Release on Delivery
Expected at 2:00 p.m. EDT
Thursday, July 12, 2007

CRITICAL INFRASTRUCTURE

Sector Plans Complete and Sector Councils Evolving

Statement of Eileen R. Larence, Director
Homeland Security and Justice Issues

July 12, 2007

CRITICAL INFRASTRUCTURE

Sector Plans Complete and Sector Councils Evolving

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-1075T, a testimony before the Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate

Why GAO Did This Study

As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures—both physical and cyber—have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is privately owned, it is vital that public and private stakeholders work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy and has promoted the formation of government and private councils for the 17 infrastructure sectors as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP).

This testimony is based primarily on GAO's July 2007 report on the sector-specific plans and the sector councils. Specifically, it addresses (1) the extent to which the sector-specific plans meet requirements, (2) the council members' views on the value of the plans and DHS's review process, and (3) the key success factors and challenges that the representatives encountered in establishing and maintaining their councils. In conducting the previous work, GAO reviewed 9 of the 17 draft plans and conducted interviews with government and private sector representatives of the 32 councils, 17 government and 15 private sector.

www.gao.gov/cgi-bin/getrpt?GAO-07-1075T.

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

Although the nine sector-specific plans GAO reviewed generally met NIPP requirements and DHS's sector-specific plan guidance, eight did not describe any incentives the sector would use to encourage owners to conduct voluntary risk assessments, as required by the NIPP. Most of the plans included the required elements of the NIPP risk management framework. However, the plans varied in how comprehensively they addressed not only their physical assets, systems, and functions, but also their human and cyber assets, systems and functions, a requirement in the NIPP, because the sectors had differing views on the extent to which they were dependent on each of these assets. A comprehensive identification of all three categories of assets is important, according to DHS plan guidance, because it provides the foundation on which to conduct risk analyses and identify appropriate protective actions. Given the disparity in the plans, it is unclear the extent to which DHS will be able to use them to identify security gaps and critical interdependencies across the sectors. DHS officials said that to determine this, they will need to review the sectors' annual reports.

Representatives of the government and sector coordinating councils had differing views regarding the value of sector-specific plans and DHS's review of those plans. While 10 of the 32 council representatives GAO interviewed reported that they saw the plans as being useful for their sectors, representatives of eight councils disagreed because they believed the plans either did not represent a partnership among the necessary key stakeholders, especially the private sector or were not valuable because the sector had already progressed beyond the plan. In addition, representatives of 11 of the 32 councils felt the review process was too lengthy, but 8 thought the review process worked well. The remaining council representatives did not offer views on these issues.

As GAO reported previously, representatives continued to report that their sector councils had preexisting relationships that helped them establish and maintain their sector councils. However, seven of the 32 representatives reported continuing difficulty achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. Eleven council representatives reported continuing difficulties sharing information between the public and private sectors as a challenge, and six council representatives expressed concerns about the viability of the information system DHS intends to rely on to share information about critical infrastructure issues with the sectors or the effectiveness of the Protected Critical Infrastructure Information program—a program that established procedures for the receipt, care, and storage of information submitted to DHS. GAO has outstanding recommendations addressing this issue, with which DHS generally agreed and is in the process of implementing.

Mr. Chairman, Ranking Member and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on infrastructure protection issues. 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 infrastructure damage and resulting chaos disrupted government and business functions alike, producing cascading effects far beyond the physical location of the storm. In 2004, authorities thwarted a terrorist plot to target financial institutions in New York. In 2005, suicide bombers struck London's public transportation system, disrupting the city's transportation and mobile telecommunications infrastructure. Our 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—continue to be vulnerable to a wide variety of threats. Because the private sector owns approximately 85 percent of the nation's critical infrastructure and key resources—banking and financial institutions, telecommunications networks, and energy production and transmission facilities, among others—it is vital that the public and private sectors form effective partnerships to successfully protect these assets.[1]

The Department of Homeland Security (DHS) is a key player in these partnerships. The Homeland Security Act of 2002 created DHS, giving the department wide-ranging responsibilities for leading and coordinating the overall national critical infrastructure protection effort.[2] The act required DHS to (1) develop a comprehensive national plan for securing the nation's critical infrastructures and key resources and (2) recommend measures to protect critical infrastructure and key resources. Homeland Security Presidential Directive 7 (HSPD-7) further defined critical infrastructure protection responsibilities for DHS and those federal agencies—known as sector-specific agencies—responsible for particular

[1]"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, 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 statement, we will use the term "critical infrastructure" to also include key resources.

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

industry sectors, such as transportation, energy, and communications. Under HSPD-7, DHS is to establish uniform policies, approaches, guidelines, and methodologies to help ensure that critical infrastructure within and across the 17 infrastructure sectors is protected.[3] The directive further promotes the use of a risk management approach to coordinate protection efforts. This approach 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.

In addition, HSPD-7 required DHS to develop a comprehensive and integrated plan for securing the nation's critical infrastructures that outlines national protection goals, objectives, milestones, and key initiatives necessary to fulfilling these responsibilities. In response, DHS developed the National Infrastructure Protection Plan (NIPP). Issued in June 2006, the NIPP is a base plan that is to serve as a road map for how DHS and other relevant stakeholders, such as owners and operators of key critical infrastructure, should use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion. In particular, the NIPP—along with more detailed guidance issued by DHS—required the individual sector-specific agencies, working with relevant government and private representatives, to submit sector-specific plans to DHS by the end of December 2006. The plans, which were released on May 21, 2007, were to establish the means by which the sectors will identify their critical assets, assess risks of terrorist attacks or other hazards to these assets, assess and prioritize those assets which have national significance, and develop protective measures for the sectors. The NIPP also requires that sector-specific agencies develop annual reports that discuss the sectors' status in implementing the plans. According to the NIPP, DHS is to use these individual plans and reports to develop an annual cross-sector report, due each September, that evaluates whether gaps exist in the protection plans and actions to be taken to protect critical infrastructures on a national level. If gaps exist, DHS is to work with the sectors to address them.

[3]These infrastructure sectors include agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, materials, and waste; communications; 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 health care; and transportation systems.

To protect critical infrastructure, the NIPP describes a partnership model as the primary means of coordinating government and private efforts. For each of the 17 sectors, the model requires formation a government coordinating council—composed of representatives of federal, state, local, or tribal agencies with purview over critical assets. The model encourages voluntary formation of a sector coordinating council—composed of representative owner-operators of these critical assets (some of which may be state or local agencies) or their respective trade associations. There are a total of 32 coordinating councils, 17 government and 15 private sector.[4] These councils create the structure through which respective groups from all levels of government and the private sector are to collaborate in developing the sector-specific plans and implementing efforts to protect critical infrastructure. The sector coordinating councils are envisioned as a primary point of contact for government to plan the entire range of infrastructure protection activities unique to the sector. In addition, the NIPP also identified cross-sector councils that are to promote coordination, communications, and the sharing of key practices across the sectors.

This statement discusses (1) the extent to which the sector-specific plans meet NIPP and DHS requirements, (2) the government and sector coordinating council members' views on the value of the plans and DHS's review process, and (3) the key success factors and challenges that sector representatives reported they encountered in establishing and maintaining their councils. My comments today are based on our July 2007 report on the sector-specific plans and sector councils.[5] Our July report was based on a review of the NIPP as well as the sector-specific plan guidance to ascertain the elements required in the plans. We also obtained and reviewed 9 of the 17 draft plans against the criteria in the NIPP and plan guidance.[6] For more detail on the criteria we used, see appendix I. We

[4]The government facilities and the national monuments and icons sectors do not have sector councils because they do not have private sector counterparts.

[5]GAO, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, GAO-07-706R (Washington, D.C.: July 10, 2007).

[6]We selected the nine plans to obtain a range of plans based on sector characteristics, such as the maturity—sectors with pre-existing relationships and a history of working together—and diversity of the sector. The plans we reviewed were banking and finance, communications, defense industrial base, energy, public health and healthcare, information technology (IT), national monuments and icons, transportation systems, and drinking water and water treatment systems. According to DHS officials, differences between these draft plans and the final plans issued on May 21, 2007, were insignificant.

conducted structured interviews with representatives of the 17 government coordinating councils and the 15 sector coordinating councils to obtain views on the value of the plans and the review process as well as the key success factors and challenges the sectors reported that they had encountered in establishing and maintaining their councils. These interviews were conducted with lead sector-specific agency representatives for the 17 sectors: the departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security,[7] the Interior, and the Treasury and the Environmental Protection Agency, as well as with the chairs, co-chairs, or steering committee members of the 15 sector coordinating councils. We conducted our work in accordance with generally accepted government auditing standards.

In Summary

Although the nine sector-specific plans we reviewed generally met NIPP requirements and DHS's sector-specific plan guidance, eight plans did not address incentives the sectors would use to encourage owners to conduct risk assessments and some plans were more comprehensive than others when discussing their physical, human, and cyber assets, systems, and functions. Most of the plans included the required elements of the NIPP risk management framework, such as security goals; and the methods the sectors expect to use to prioritize infrastructure as well as to develop and implement protective programs and assess threats, risks, and vulnerabilities.[8] However, some plans were more developed and comprehensive, depending on the maturity of the sector and on how the sector defines its assets and functions. While all of the plans described the threat analyses that the sector conducts, eight of the plans did not describe any incentives the sector would use to encourage owners to conduct voluntary risk assessments, as required by the NIPP. These incentives are important because a number of the industries in the sectors are privately owned and not regulated, and the government must rely on voluntary compliance with the NIPP. DHS officials said that the variance in the plans can primarily be attributed to the levels of maturity and cultures of the sectors, with the more mature sectors—sectors with preexisting relationships and a history of working together—generally

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

[8]See appendix I for the required elements on which we reviewed the plans.

having more comprehensive and complete plans than more newly established sectors without similar prior relationships. The plans also varied in how comprehensively they addressed not only their physical assets, systems, and functions,[9] but also their human and cyber assets, systems, and functions, a requirement in the NIPP, because the sectors reported that they had differing views on the extent to which they were dependent on each of these assets. A comprehensive identification of all three categories of assets is important, according to DHS sector-specific plan guidance, because such analysis provides the foundation on which to conduct risk analyses and identify the appropriate mix of protective programs and actions that will most effectively reduce the risk to the nation's infrastructure. Yet, only one of the plans—drinking water and water treatment systems—included all three categories of assets. For example, because the communications sector limited its definition of assets to networks, systems, and functions, it did not, as required by DHS plan guidance, discuss how human assets fit into existing security projects or are relevant to fill the gaps to meet the sector's security goals. DHS's Office of Infrastructure Protection officials acknowledged the differences in how comprehensive the plans are, but said that these initial plans are only a first step and that they will work with the sectors to address differences in future updates. Given the disparity in the plans, however, it is unclear the extent to which DHS will be able to use them at this point to identify security gaps and critical interdependencies across the sectors in order to plan future protective measures. From reviewing these plans, it is also unclear how far along each sector actually is in identifying assets, setting priorities, and developing activities to protect key assets. DHS officials said that to determine this, they will need to review the sectors' annual progress reports, due this month, that are to provide additional implementation information.

Representatives of the government and sector coordinating councils had differing views regarding the value of sector-specific plans and DHS's review of those plans. While 10 of the 32 council representatives we interviewed reported that they saw the plans as useful for the sector, representatives of eight councils disagreed because they believed the plans either did not represent a partnership among the necessary key stakeholders, especially the private sector, or were not valuable because

[9]In the context of the NIPP, a "system" is a collection of assets, resources, or elements that perform a process that provides infrastructure services to the nation. A "function" is defined as the service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

the sector had already done so much work on its own and had progressed beyond the plan. For example, the government facilities council representative said that the plan was useful because relationships across the sector were established during its development that have resulted in enhanced coordination of previously disjointed security efforts. DHS's Office of Infrastructure Protection officials agreed that the main benefit of the plans was that the process of developing them helped the sectors establish relationships between the private sector and the government and among private sector stakeholders. In contrast, the representative from the nuclear reactors, materials, and waste sector's coordinating council said that because the sector's security has been robust for a long time, the plan only casts the security of the sector in a different light. Also, the drinking water and water treatment sector representative said that the plan did not provide added value for the sector because the sector already has a 30-year history of protection. DHS Office of Infrastructure Protection officials acknowledged that these sectors have a long history of relationships with the federal government and in some cases have been doing similar planning efforts and said that while the NIPP planning process may not have been as valuable to these sectors, it was valuable to DHS to have plans for all critical infrastructure sectors. Representatives of 11 of 32 councils felt that the review process was too lengthy and said that they had turned in their plans in advance of the December 31, 2006, deadline established by the NIPP, but had to wait more than 5 months for the plans to be approved. DHS's Infrastructure Protection officials agreed that the review process had been lengthy and that time periods allowed for the sectors to respond to comments were too short. The officials said this occurred because of the volume of work DHS had to undertake and because some of the sector specific agencies did not communicate well with the sectors since they were still learning to operate effectively with the private sector, treating it as an equal partner under the NIPP model. The officials said that they plan to refine the process as the sector-specific agencies gain more experience working with the private sector. Conversely, representatives from eight of 32 councils said the review process for the plans worked well, despite the time it took, and five council representatives were complimentary of the support they received from DHS. The remaining council representatives did not offer views on these issues.

As we reported last year,[10] long-standing relationships were frequently cited as most helpful in establishing councils. Council representatives for 9 of the 32 councils continued to cite preexisting relationships as helping them in establishing and maintaining their sector councils, and two sectors noted that going through the process of establishing the councils had, in turn, improved relationships, while seven said achieving the necessary participation in the council is a continuing challenge. For example, the dams, energy, and banking and finance sectors, among others, said that existing relationships continue to help in maintaining their councils. On the other hand, seven sector council representatives reported difficulty in achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. For example, the public health and health care sector representative said that getting sector members to participate is a challenge and noted that because of this, the first step in implementing the sector-specific plan is to increase awareness about the council. In addition, 11 of the 32 council representatives reported continuing difficulties with sharing information between the public and private sectors as a challenge. Furthermore, 6 of the 32 council representatives expressed concerns about the viability of the information system—the Homeland Security Information Network (HSIN)—DHS intends to rely on to share information with the sectors about critical infrastructure issues, as well as the effectiveness of the Protected Critical Infrastructure Information (PCII) program—a program that established procedures for the receipt, care, and storage of information submitted to DHS. Although encouraging the sectors to use HSIN, DHS's Infrastructure Protection officials said the system does not provide the capabilities that were promised, including providing the level of security expected by some sectors. Relatedly, in April 2007, we reported that the HSIN system was built without appropriate coordination with other information-sharing initiatives.[11] Additionally, as we have reported,[12] potential submitters under the PCII program continue to fear that the information, such as information on security vulnerabilities, could be inadequately protected,

[10]GAO, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39 (Washington, D.C.: Oct. 16, 2006).

[11]GAO, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*, GAO-07-455 (Washington, D.C.: Apr. 16, 2007).

[12]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).

used for future legal or regulatory action, or inadvertently released. We previously recommended that, among other things, DHS better (1) define its critical infrastructure information needs and (2) explain how this information will be used to attract more users. DHS concurred with our recommendations. In September 2006, DHS issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS. DHS is in the process of implementing our additional recommendations that it better define its critical-infrastructure information needs under the PCII program and better explain how this information will be used to build the private sector's trust and attract more users.

Background

DHS serves as the sector-specific agency for 10 of the sectors: information technology; communications; transportation systems; chemical; emergency services; nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities. Other sector-specific agencies are the departments of Agriculture, Defense, Energy, Health and Human Services, the Interior, the Treasury, and the Environmental Protection Agency. (See table 1 for a list of sector-specific agencies and a brief description of each sector).

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

Sector-specific agency	Sector	Description
Departments of Agriculture,[a] and Health and Human Services, Food and Drug Administration[b]	Agriculture and food	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production. Carries out the postharvesting of the food supply, including processing and retail sales.
Department of Defense	Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Department of Energy	Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.
Department of Health and Human Services	Public health and health care	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.
Department of the Interior	National monuments and icons	Memorializes or represents monuments, physical structures, objects, or geographical sites that are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance.
Department of the Treasury	Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.
Environmental Protection Agency	Drinking water and water treatment systems	Provides sources of safe drinking water from more than 53,000 community water systems and properly treated wastewater from more than 16,000 publicly owned treatment works.
Department of Homeland Security:		
Office of Infrastructure Protection	Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
	Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.
	Dams	Manages water retention structures, including levees, more than 77,000 conventional dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.
	Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.

Sector-specific agency	Sector	Description
	Nuclear reactors, materials, and waste	Provides nuclear power, which accounts for approximately 20 percent of the nation's electrical generating capacity. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.
Office of Cyber Security and Communications	Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.
	Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.
Transportation Security Administration	Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.
Transportation Security Administration and U.S. Coast Guard	Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.
Immigration and Customs Enforcement, Federal Protective Service	Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

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

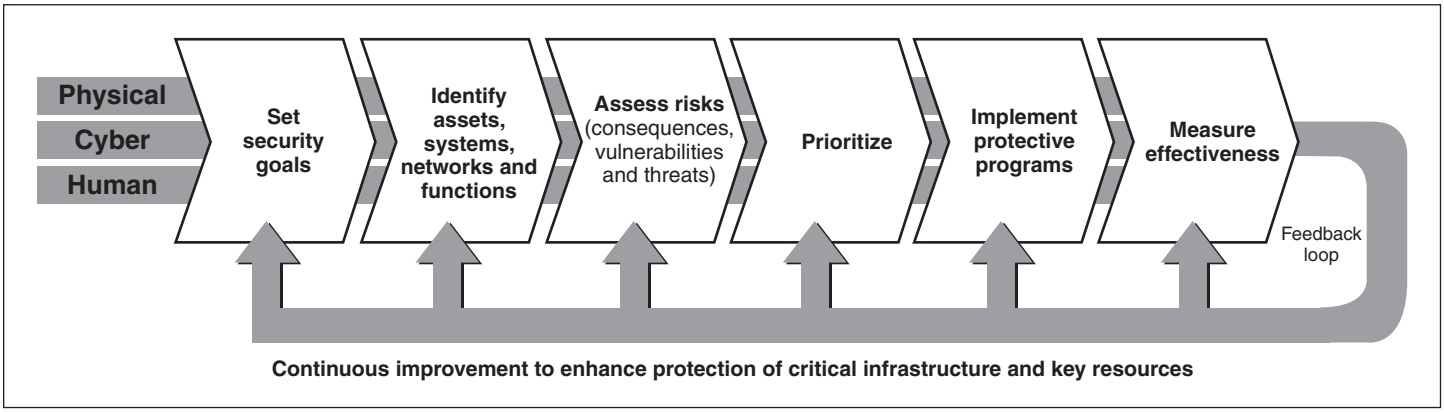
[a]The Department of Agriculture is responsible for food (including meat, poultry, and eggs) and agriculture.

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

Most Sector Plans We Reviewed Met NIPP and DHS Sector-Specific Plan Guidance, but Varied Depending on Their Maturity and How They Define Their Assets

The nine sector-specific plans we reviewed generally met NIPP requirements and DHS's sector-specific plan guidance; however, the extent to which the plans met this guidance, and therefore their usefulness in enabling DHS to identify gaps and interdependencies across the sectors, varied depending on the maturity of the sector and on how the sector defines its assets, systems, and functions. As required by the NIPP risk management framework (see fig. 1), sector-specific plans are to promote the protection of physical, cyber, and human assets by focusing activities on efforts to (1) set security goals; (2) identify assets, systems, networks, and functions; (3) assess risk based on consequences, vulnerabilities, and threats;[13] (4) establish priorities based on risk assessments; (5) implement protective programs; and (6) measure effectiveness.

Figure 1: NIPP Risk Management Framework



Source: Department of Homeland Security: National Infrastructure Protection Plan.

In addition to these NIPP risk management plan elements outlined above and according to DHS's sector-specific plan guidance, the plans are also to address the sectors' efforts to (1) implement a research and development program for critical infrastructure protection and (2) establish a structure

[13]According to the NIPP, a "consequence" is the result of a terrorist attack or hazard that reflects the level, duration, and nature of the loss resulting from the incident. A "vulnerability" is a weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary or disrupted by a natural hazard or technological failure. A "threat" is the intention and capability of an adversary to undertake actions that would be detrimental to critical infrastructure and key resources.

for managing and coordinating the responsibilities of the federal departments and agencies—otherwise known as sector-specific agencies—identified in HSPD-7 as responsible for critical-infrastructure protection activities specified for the 17 sectors.[14] Most of the plans included the required elements of the NIPP risk management framework, such as security goals and the methods the sectors expect to use to prioritize infrastructure, as well as to develop and implement protective programs. However, the plans varied in the extent to which they included key information required for each plan element. For example, all of the plans described the threat analyses that the sector conducts, but only one of the plans described any incentives used to encourage voluntary risk assessments, as required by the NIPP. Such incentives are important because a number of the industries in the sectors are privately owned and not regulated, and the government must rely on voluntary compliance with the NIPP. Additionally, although the NIPP called for each sector to identify key protective programs, three of the nine plans did not address this requirement. DHS officials told us that this variance in the plans can, in large part, be attributed to the levels of maturity and cultures of the sectors, with the more mature sectors generally having more comprehensive and complete plans than sectors without similar prior working relationships. For example, the banking and finance and energy sector plans included most of the key information required for each plan element. According to DHS officials, this is a result of these sectors having a history and culture of working with the government to plan and accomplish many of the same activities that are being required for the sector-specific plans. Therefore, these sectors were able to create plans that were more comprehensive and developed than those of less mature sectors, such as the public health and health care and agriculture and food sectors.

The plans also varied in how comprehensively they addressed their physical, human, and cyber assets, systems, and functions because sectors reported having differing views on the extent to which they were dependent on each of these assets, systems, and functions. According to DHS's sector-specific plan guidance, a comprehensive identification of such assets is important because it provides the foundation on which to conduct risk analysis and identify the appropriate mix of protective programs and actions that will most effectively reduce the risk to the nation's infrastructure. Yet, only one of the plans—drinking water and

[14]See appendix I for a full list of the requirements on which we evaluated the plans.

water treatment—specifically included all three categories of assets. For example, because the communications sector limited its definition of assets to networks, systems, and functions, it did not, as required by DHS's plan guidance, include human assets in its existing security projects and the gaps it needs to fill related to these assets to support the sector's goals. In addition, the national monuments and icons plan defined the sector as consisting of physical structures with minimal cyber and telecommunications assets because these assets are not sufficiently critical that damaging or destroying them would interfere with the continued operation of the physical assets. In contrast, the energy sector placed a greater emphasis on cyber attributes because it heavily depends on these cyber assets to monitor and control its energy systems. DHS officials also attributed the difference in the extent to which the plans addressed required elements to the manner in which the sectors define their assets and functions.

The plans, according to DHS's Office of Infrastructure Protection officials, are a first step in developing future protective measures. In addition, these officials said that the plans should not be considered to be reports of actual implementation of such measures. Given the disparity in the plans, it is unclear the extent to which DHS will be able to use them to identify gaps and interdependencies across the sectors in order to plan future protective measures. It is also unclear, from reviewing the plans, how far along each sector actually is in identifying assets, setting priorities, and protecting key assets. DHS officials said that to make this determination, they will need to review the sectors' annual progress reports, due in this month, that are to provide additional information on plan implementation as well as identify sector priorities.

Council Representatives Disagreed on the Value of the Plans and the Review Process

Representatives of 10 of 32 councils said the plans were valuable because they gave their sectors a common language and framework to bring the disparate members of the sector together to better collaborate as they move forward with protection efforts. For example, the government facilities council representative said that the plan was useful because relationships across the sector were established during its development that have resulted in bringing previously disjointed security efforts together in a coordinated way. The banking and finance sector's coordinating council representative said that the plan was a helpful way of documenting the history, the present state, and the future of the sector in a way that had not been done before and that the plan will be a working document to guide the sector in coordinating efforts. Similarly, an energy sector representative said that the plan provides a common format so that

all participants can speak a common language, thus enabling them to better collaborate on the overall security of the sector. The representative also said that the plan brought the issue of interdependencies between the energy sector and other sectors to light and provided a forum for the various sectors to collaborate. DHS's Office of Infrastructure Protection officials agreed that the main benefit of these plans was that the process of developing them helped the sectors to establish relationships between the private sector and the government and among private sector stakeholders that are key to the success of protection efforts.

However, representatives of 8 of the 32 councils said the plans were not useful to their sectors because (1) the plans did not represent a true partnership between the federal and private sectors or were not meaningful to all the industries represented by the sector or (2) the sector had already taken significant protection actions, thus, developing the plan did not add value. The remaining council representatives did not offer views on this issue. Sector representatives for three transportation modes—rail, maritime, and aviation—reported that their sector's plan was written by the government and that the private sector did not participate fully in the development of the plan or the review process. As a result, the representatives did not believe that the plan was of value to the transportation sector as a whole because it does not represent the interests of the private sector. Similarly, agriculture and food representatives said writing the plan proved to be difficult because of the sector's diversity and size—more than 2,000,000 farms, one million restaurants, and 150,000 meat processing plants. They said that one of the sector's biggest challenges was developing a meaningful document that could be used by all of the industries represented. As a result of these challenges, the sector submitted two plans in December 2006 that represented a best effort at the time, but the sector council said it intends to use the remainder of the 2007 calendar year to create a single plan that better represents the sector. In contrast, the coordinating council representative for nuclear reactors, materials, and waste sector said that because the sector's security has been robust for a long time, the plan only casts the security of the sector in a different light, and the drinking water and water treatment systems sector said that the plan is a "snapshot in time" document for a sector that already has a 30-year history of protection, and thus the plan did not provide added value for the sector. Officials at DHS's Office of Infrastructure Protection acknowledged that these sectors have a long history of working together and in some cases have been doing similar planning efforts. However, the officials said that the effort was of value to the government because it now has plans for all

17 sectors and it can begin to use the plans to address the NIPP risk management framework.

Representatives of 11 of 32 councils said the review process associated with the plans was lengthy. They commented that they had submitted their plans in advance of the December 31, 2006, deadline, but had to wait 5 months for the plan to be approved. Eight of them also commented that while they were required to respond within several days to comments from DHS on the draft plans, they had to wait relatively much longer during the continuing review process for the next iteration of the draft. For example, a representative of the drinking water and water treatment sector said that the time the sector had to incorporate DHS's comments into a draft of the plan was too short—a few days—and this led the sector to question whether its members were valued partners to DHS. DHS's Infrastructure Protection officials agreed that the review process had been lengthy and that the comment periods given to sector officials were too short. DHS officials said this occurred because of the volume of work DHS had to undertake and because some of the sector-specific agencies were still learning to operate effectively with the private sector under a partnership model in which the private sector is an equal partner. The officials said that they plan to refine the process as the sector-specific agencies gain more experience working with the private sector.

Conversely, representatives from eight of 32 councils said the review process for the plans worked well, and five of these council representatives were complimentary of the support they received from DHS. The remaining council representatives did not offer views on this topic. For example, an information technology (IT) sector coordinating council representative said that the review and feedback process on their plan worked well and that the Office of Infrastructure Protection has helped tremendously in bringing the plans to fruition. However, sector coordinating council representatives for six sectors also voiced concern that the trusted relationships established between the sectors and DHS might not continue if there were additional turnover in DHS, as has occurred in the past. For example, the representative of one council said they had established productive working relationships with officials in the Offices of Infrastructure Protection and Cyber Security and Communications, but were concerned that these relationships were dependent on the individuals in these positions and that the relationships may not continue without the same individuals in charge at DHS. As we

have reported in the past, developing trusted partnerships between the federal government and the private sector is critical to ensure the protection of critical infrastructure.[15]

Long-standing Relationships Continue to Facilitate Councils, but Some Council Representatives Reported Information-Sharing Challenges

Nine of 32 sector representatives said that their preexisting relationships with stakeholders helped in establishing and maintaining their sector councils, and two noted that establishing the councils had improved relationships. Such participation is critical to well-functioning councils. For example, representatives from the dams, energy, and banking and finance sectors, among others, said that existing relationships continue to help in maintaining their councils. In addition, the defense industrial base representatives said the organizational infrastructure provided by the sector councils is valuable because it allows for collaboration. Representatives from the national monuments and icons sector said that establishing the government sector council has facilitated communication within the sector. We also reported previously that long-standing relationships were a facilitating factor in council formation and that 10 sectors had formed either a government council or sector council that addressed critical infrastructure protection issues prior to DHS's development of the NIPP.[16] As a result, these 10 sectors were more easily able to establish government coordinating councils and sector coordinating councils under the NIPP model. Several councils also noted that the Critical Infrastructure Partnership Advisory Council (CIPAC), created by DHS in March 2006 to facilitate communication and information sharing between the government and the private sector, has helped facilitate collaboration because it allows the government and industry to interact without being open to public scrutiny under the Federal Advisory Committee Act.[17] This is important because previously,

[15]GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004) and *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[16]See GAO-07-39.

[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). Section 871 of the Homeland Security Act authorized a process under which the Secretary could exempt an advisory committee from the Federal Advisory Committee Act. See Pub. L. No. 107-296, § 871, 116 Stat. 2135, 2243.

meetings between the private sector and the government had to be open to the public, hampering the private sector's willingness to share information.

Conversely, seven sector council representatives reported difficulty in achieving and maintaining sector council membership, thus limiting the ability of the councils to effectively represent the sector. For example, the public health and health care sector representative said that getting the numerous sector members to participate is a challenge, and the government representative noted that because of this, the first step in implementing the sector-specific plan is to increase awareness about the effort among sector members to encourage participation. Similarly, due to the size of the commercial facilities sector, participation, while critical, varies among its industries, according to the government council representative. Meanwhile, the banking and finance sector representatives said that the time commitment for private sector members and council leaders makes participation difficult for smaller stakeholders, but getting them involved is critical to an effective partnership. Likewise, the IT sector representatives said engaging some government members in joint council meetings is a continuing challenge because of the members' competing responsibilities. Without such involvement, the officials said, it is difficult to convince the private sector representatives of the value of spending their time participating on the council.

Additionally, obtaining state and local government participation in government sector councils remains a challenge for five sectors. Achieving such participation is critical because these officials are often the first responders in case of an incident. Several government council representatives said that a lack of funding for representatives from these entities to travel to key meetings has limited state and local government participation. Others stated that determining which officials to include was a challenge because of the sheer volume of state and local stakeholders. DHS Infrastructure Protection officials said that the agency is trying to address this issue by providing funding for state and local participation in quarterly sector council meetings and has created a State, Local and Tribal and Territorial Government Coordinating Council (SLTTGCC)—composed of state, local, tribal, and territorial homeland security advisers—that serves as a forum for coordination across these jurisdictions on protection guidance, strategies, and programs.

Eleven of the 32 council representatives reported continuing challenges with sharing information between the federal government and the private sector. For example, six council representatives expressed concerns about the viability of two of DHS's main information-sharing tools—the

Homeland Security Information Network (HSIN) or the Protected Critical Infrastructure Information (PCII) program. We reported in April 2007 that the HSIN system was built without appropriate coordination with other information-sharing initiatives.[18] In addition, in a strategic review of HSIN, DHS reported in April 2007 that it has not clearly defined the purpose and scope of HSIN and that HSIN has been developed without sufficient planning and program management. According to DHS Infrastructure Protection officials, although they encouraged the sectors to use HSIN, the system does not provide the capabilities that were promised, including providing the level of security expected by some sectors. As a result, they said the Office of Infrastructure Protection is exploring an alternative that would better meet the needs of the sectors. In addition, three council representatives expressed concerns about whether information shared under the PCII program would be protected. Although this program was specifically designed to establish procedures for the receipt, care, and storage of critical infrastructure information submitted voluntarily to the government, the representatives said potential submitters continue to fear that the information could be inadequately protected, used for future legal or regulatory action, or inadvertently released.

In April 2006, we reported that DHS faced challenges implementing the program, including being able to assure the private sector that submitted information will be protected and specifying who will be authorized to have access to the information, as well as to demonstrate to the critical infrastructure owners the benefits of sharing the information to encourage program participation.[19] We recommended, among other things, that DHS better (1) define its critical-infrastructure information needs and (2) explain how this information will be used to attract more users. DHS concurred with our recommendations. In September 2006 DHS issued a final rule that established procedures governing the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS. DHS is in the process of implementing our additional recommendations that it define its critical-infrastructure information needs under the PCII program and better explain how this information will be used to build the private sector's trust and attract more users.

[18]See GAO-07-455.

[19]See GAO-06-383.

Concluding Observations

To date, DHS has issued a national plan aimed at providing a consistent approach to critical infrastructure protection, ensured that all 17 sectors have organized to collaborate on protection efforts, and worked with government and private sector partners to complete all 17 sector-specific plans. Nevertheless, our work has shown that sectors vary in terms of how complete and comprehensive their plans are. Furthermore, DHS recognizes that the sectors, their councils, and their plans must continue to evolve. As they do and as the plans are updated and annual implementation reports are provided that begin to show the level of protection achieved, it will be important that the plans and reports add value, both to the sectors themselves and to the government as a whole. This is critical because DHS is dependent on these plans and reports to meet its mandate to evaluate whether gaps exist in the protection of the nation's most critical infrastructure and key resources and, if gaps exist, to work with the sectors to address the gaps. Likewise, DHS must depend on the private sector to voluntarily put protective measures in place for many assets. It will also be important that sector councils have representative members and that the sector-specific agencies have buy-in from these members on protection plans and implementation steps. One step DHS could take to implement our past recommendations to strengthen the sharing of information is for the PCII program to better define its critical infrastructure information needs and better explain how this information will be used to build the private sector's trust and attract more users. As we have previously reported, such sharing of information and the building of trusted relationships are crucial to the protection of the nation's critical infrastructure.

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

Contact Information

For further information on this testimony, please contact Eileen Larence at (202) 512-8777 or by e-mail at larencee@gao.gov. Individuals making key contributions to this testimony include Susan Quinlan, Assistant Director; R. E. Canjar; Landis Lindsey; E. Jerry Seigler; and Edith Sohna.

Appendix I: Criteria Used to Determine Completeness of Sector Specific Plans

We assessed the sector specific plans (SSPs) using 8 criteria, consisting of 40 key information requirements. We extracted this information from the requirements included in the NIPP as well as on the detailed sector-specific plan guidance issued by DHS. Each criterion reflects a component DHS required for the completion of the SSP. The 8 criteria we used are listed below along with the corresponding 40 key information requirements.

Section 1: Sector Profile and Goals

1. Did the sector include physical and human assets as part of its sector profile?[1]

2. Does the SSP identify any regulations or key authorities relevant to the sector that affect physical and human assets and protection?

3. Does the SSP show the relationships between the sector specific agency and the private sector, other federal departments and agencies, and state and local agencies that are either owner/operators of assets or provide a supporting role to securing key resources?

4. Does the SSP contain sector-specific goals?

5. Does the SSP communicate the value of the plan to the private sector, other owners, and operators?

Section 2: Identify Assets, Systems, Networks, and Functions

6. Does the SSP include a process for identifying the sector's assets and functions, both now and in the future?

7. Does the SSP include a process to identify physical and human asset dependencies and interdependencies?

8. Does the SSP describe the criteria being used to determine which assets, systems, and networks are and are not of potential concern?

9. Does the SSP describe how the infrastructure information being collected will be verified for accuracy and completeness?

[1]A companion engagement assessed the plans for inclusion of cyber assets.

Section 3: Assess Risks

10. Does the SSP discuss the risk assessment process, including whether the sector is mandated by regulation or are primarily voluntary in nature.

11. Does the SSP address whether a screening process (process to determine whether a full assessment is required) for assets would be beneficial for the sector, and if so, does it discuss the methodologies or tools that would be used to do so?

12. Does the SSP identify how potential consequences of incidents, including worst case scenarios, would be assessed?

13. Does the SSP describe the relevant processes and methodologies used to perform vulnerability assessments?

14. Does the SSP describe any threat analyses that the sector conducts?

15. Does the SSP describe any incentives used to encourage voluntary performance of risk assessments?

Section 4: Prioritize Infrastructure

16. Does the SSP identify the party responsible for conducting a risk-based prioritizing of the assets?

17. Does the SSP describe the process, current criteria, and frequency for prioritizing sector assets?

18. Does the SSP provide a common methodology for comparing both physical and human assets when prioritizing a sector's infrastructure?

Section 5: Develop and Implement Protective Programs

19. Does the SSP describe the process that the SSA will use to work with asset owners to develop effective long-term protective plans for the sector's assets?

20. Does the SSP identify key protective programs (and their role) in the sector's overall risk management approach?

21. Does the SSP describe the process used to identify and validate specific program needs?

22. Does the SSP include the minimum requirements necessary for the sector to prevent, protect, respond to, and recover from an attack?

23. Does the SSP address implementation and maintenance of protective programs for assets once they are prioritized?

24. Does the SSP address how the performance of protective programs is monitored by the sector-specific agencies and security partners to determine their effectiveness?

Section 6: Measure Progress

25. Does the SSP explain how the SSA will collect, verify and report the information necessary to measure progress in critical infrastructure/key resources protection?

26. Does the SSP describe how the SSA will report the results of its performance assessments to the Secretary of Homeland Security?

27. Does the SSP call for the development and use of metrics that will allow the SSA to measure the results of activities related to assets?

28. Does the SPP describe how performance metrics will be used to guide future decisions on projects?

29. Does the SSP list relevant sector-level implementation actions that the SSA and its security partners deem appropriate?

Section 7: Research and Development for Critical Infrastructure/Key Resources Protection

30. Does the SSP describe how technology development is related to the sector's goals?

31. Does the SSP identify those sector capability requirements that can be supported by technology development?

32. Does the SSP describe the process used to identify physical and human sector-related research requirements?

33. Does the SSP identify existing security projects and the gaps it needs to fill to support the sector's goals?

34. Does the SSP identify which sector governance structures will be responsible for R&D?

35. Does the SSP describe the criteria that are used to select new and existing initiatives?

Section 8: Manage and Coordinate SSA Responsibilities

36. Does the SSP describe how the SSA intends to staff and manage its NIPP responsibilities? (e.g., creation of a program management office.)

37. Does the SSP describe the processes and responsibilities of updating, reporting, budgeting, and training?

38. Does the SSP describe the sector's coordinating mechanisms and structures?

39. Does the SSP describe the process for developing the sector-specific investment priorities and requirements for critical infrastructure/key resource protection?

40. Does the SSP describe the process for information sharing and protection?

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