United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2010

CRITICAL INFRASTRUCTURE PROTECTION

DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened

GAO-10-772

September 2010

CRITICAL INFRASTRUCTURE PROTECTION

DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-772, a report to congressional requesters

Why GAO Did This Study

According to the Department of Homeland Security (DHS), protecting and ensuring the resiliency (the ability to resist, absorb, recover from, or successfully adapt to adversity or changing conditions) of critical infrastructure and key resources (CIKR) is essential to the nation's security. By law, DHS is to lead and coordinate efforts to protect several thousand CIKR assets deemed vital to the nation's security, public health, and economy. In 2006, DHS created the National Infrastructure Protection Plan (NIPP) to outline the approach for integrating CIKR and increased its emphasis on resiliency in its 2009 update. GAO was asked to assess the extent to which DHS (1) has incorporated resiliency into the programs it uses to work with asset owners and operators and (2) is positioned to disseminate information it gathers on resiliency practices to asset owners and operators. GAO reviewed DHS documents, such as the NIPP, and interviewed DHS officials and 15 owners and operators of assets selected on the basis of geographic diversity. The results of these interviews are not generalizable but provide insights.

What GAO Recommends

GAO recommends that DHS develop resiliency performance measures, update Protective Security Advisor (PSA) guidelines, and determine the feasibility of developing an approach to disseminate resiliency information. DHS is taking action to implement two recommendations and is internally considering the third.

View GAO-10-772 or key components.
For more information, contact Stephen L. Caldwell at (202) 512-8777 or caldwells@gao.gov.

What GAO Found

DHS's efforts to incorporate resiliency into the programs it uses to work with asset owners and operators is evolving but program management could be strengthened. Specifically, DHS is developing or updating programs to assess vulnerability and risk at CIKR facilities and within groups of related infrastructure, regions, and systems to place greater emphasis on resiliency. However, DHS has not taken commensurate efforts to measure asset owners' and operators' actions to address resiliency gaps. DHS operates its Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists, called PSAs, to assist asset owners and operators on CIKR protection strategies, and has provided guidelines to PSAs on key job tasks such as how to establish relationships between asset owners and operators and DHS, federal, state, and local officials. DHS has provided training to PSAs on resiliency topics, but has not updated PSA guidelines to articulate the role of PSAs with regard to resiliency issues, or how PSAs are to promote resiliency strategies and practices to asset owners and operators. A senior DHS official described plans to update PSA guidelines and the intent to outline this plan in October 2010, but did not provide information on what changes would be made to articulate PSA roles and responsibility with regard to resiliency. By developing measures to assess the extent to which asset owners and operators are addressing resiliency gaps and updating PSA guidance, DHS would be better positioned to manage its efforts to help asset owners and operators enhance their resiliency.

DHS faces barriers disseminating information about resiliency practices across the spectrum of asset owners and operators. DHS shares information on potential protective measures with asset owners and operators and others including state and local officials (generally on a case-by-case basis) after it has completed vulnerability assessments at CIKR facilities. DHS officials told GAO that they have considered ways to disseminate information that they collect or plan to collect with regard to resiliency. However, DHS faces barriers sharing information about resiliency strategies. For example, given the voluntary nature of the CIKR partnership, DHS officials stated that DHS should not be viewed as identifying and promoting practices which could be construed by CIKR partners to be standards. Also, according to DHS officials, the need for and the emphasis on resiliency can vary across different types of facilities depending on the nature of the facility. For example, an oil refinery is inherently different than a government office building. DHS's efforts to emphasize resiliency when developing or updating the programs it uses to work with owners and operators creates an opportunity for DHS to position itself to disseminate information about resiliency practices within and across the spectrum of asset owners and operators. By determining the feasibility of overcoming barriers and developing an approach for disseminating information on resiliency practices within and across sectors, DHS could better position itself to help asset owners and operators consider and adopt resiliency strategies.

Contents

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 23, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation Security
and Infrastructure Protection
Committee on Homeland Security
House of Representatives

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. Threats against critical infrastructure are not limited to natural disasters. For example, in 2005, suicide bombers struck London's public transportation system, disrupting the city's transportation and mobile telecommunications infrastructure. In March 2007, we reported that our nation's critical infrastructures and key resources (CIKR)—assets and systems, 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—continue to be vulnerable to a wide variety of threats.[1] According to the Department of Homeland Security (DHS), because the private sector owns the vast majority of the nation's CIKR—banking and financial institutions, telecommunications networks, and energy production and transmission facilities, among others—it is vital that the public and private sectors work together to protect these assets and systems.

The Homeland Security Act of 2002 created DHS and gave the department wide-ranging responsibilities for, among other things, leading and

[1] GAO, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors*, GAO-07-626T (Washington, D.C.: March 2007).

coordinating the overall national critical infrastructure protection effort.[2] Homeland Security Presidential Directive (HSPD)-7 further defined critical infrastructure protection responsibilities for DHS and those federal agencies—known as sector-specific agencies (SSAs)—responsible for particular CIKR sectors, such as the chemical, commercial facilities, communications, energy, and transportation sectors.[3] HSPD-7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across the 17 CIKR sectors. The directive also gave DHS the authority to establish additional sectors and in 2008, DHS established an 18th sector for critical manufacturing.

In accordance with the Homeland Security Act and in response to HSPD-7, DHS issued the first National Infrastructure Protection Plan (NIPP) in June 2006, which provides the overarching approach for integrating the nation's CIKR protection initiatives into a single national effort.[4] DHS issued a revised NIPP in January 2009.[5] The NIPP sets forth a risk management framework and details the roles and responsibilities for DHS, SSAs, and other federal, state, regional, local, tribal, territorial, and private sector partners implementing the NIPP, including how they should use risk management principles to prioritize protection activities within and across sectors.[6] Within the NIPP framework, DHS has emphasized the importance of collaboration and partnering with and among the various partners and its reliance on voluntary information sharing between the

[2] See generally Pub. L. No. 107-296, 116 Stat. 2135 (2002). Title II of the Homeland Security Act, as amended, primarily addresses the department's responsibilities for critical infrastructure protection.

[3] Homeland Security Presidential Directive Number 7 (Washington, D.C.: Dec. 17, 2003).

[4] DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).

[5] DHS, *National Infrastructure Protection Plan*, *Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

[6] The NIPP risk management framework is a planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risk based on consequences, vulnerabilities, and threats; implementing protective programs and resiliency strategies; measuring performance; and taking corrective action.

private sector and DHS.[7] The NIPP provides the framework for developing, implementing, and maintaining a coordinated national effort to protect CIKR in the 18 sectors. Each of the CIKR sectors is represented in the federal planning process by a SSA; a government coordinating council (GCC) to represent each sector's interests among government agencies; and a sector coordinating council (SCC) that includes private sector representatives of the sector.[8] Each sector is responsible for developing sector-specific plans and sector annual reports. The sector-specific plans are to provide the means by which the NIPP is implemented across the sectors, as well as a national framework for each sector that guides the development, implementation, and updating of state and local homeland security strategies and CIKR protection programs. Sector annual reports articulate the progress of the sector's CIKR protection and resiliency efforts, challenges, and needs to other sectors, government agencies, CIKR partners, the Executive Office of the President, and Congress.

As part of its risk management strategy, DHS has established a National Critical Infrastructure Prioritization Program which uses a tiered approach to identify nationally significant CIKR to enhance decision making related to CIKR protection.[9] These assets and systems can include a range of businesses or facilities in a local geographic area, such as refineries, chemical facilities, or commercial facilities, as well as the information systems and data systems that ensure their continued operation. CIKR

[7] For more information, see GAO, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, GAO-09-654R (Washington, D.C.: June 2009). Our report discussed a DHS report, developed pursuant to a congressional mandate, which analyzed whether DHS should require private sector entities to provide it with existing information about their security measures and vulnerabilities in order to improve the department's ability to evaluate critical infrastructure protection nationwide. We reported that, according to DHS, requiring private sector entities to provide sensitive information to the department conflicts with the voluntary information-sharing approach DHS was to pursue under the Homeland Security Act.

[8] The GCC is comprised of representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the security and operational landscape of each individual sector. The SCC is the private sector counterpart to the GCC. These councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key private sector stakeholders within each sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues. The Government Facilities and National Monuments and Icons Sectors do not have a GCC due to the fact that they are uniquely governmental.

[9] Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

identified through the program include several thousand level 1 or level 2 assets and systems which are those that if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity. According to DHS, the overwhelming majority of the assets and systems identified through this effort are classified as level 2. Only a small subset of assets meet the level 1 consequence threshold—those whose loss or damage could result in major national or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001 attacks.[10] We placed the protection of the federal government's information systems and the nation's critical infrastructure on our high-risk list in 1997 because the security of the information systems, networks, and data that sustain the operations of CIKR is essential to preventing disruptions in critical operations across and among CIKR.[11]

Over the last several years, various stakeholders, including members of Congress, academia, and the private sector have questioned DHS's approach to critical infrastructure protection. These stakeholders have expressed concerns that DHS has placed most of its emphasis on protection—actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with an attack or disaster—rather than resiliency—which, according to DHS, is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. In response to your request that we study DHS's revisions to the NIPP and efforts by DHS to address resiliency as part of its national planning efforts, in March 2010 we reported that DHS had increased its emphasis on the concept of critical infrastructure resiliency as a part of its national CIKR planning efforts.[12] Specifically, DHS has increased its emphasis on

[10] DHS conducts the process of identifying these nationally significant assets and systems on an annual basis and relies heavily on the insights and knowledge of a wide array of public and private sector partners. CIKR categorized as level 1 or level 2 as a result of this annual process provide a common basis on which DHS and its partners can implement important CIKR protection programs and initiatives, such as various grant programs, facility assessments and training, and other activities.

[11] In 1990, we began a program to report on government operations that we identified as "high risk." We periodically report on the progress to address these high-risk areas, generally at the start of each new Congress. For more information on the high-risk program generally, and critical infrastructure protection in particular, see GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[12] GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: March 2010).

resiliency in the most recent edition of the NIPP and has directed SSAs to address resiliency in their sector-specific plans, which SSAs intend to publish later this year.[13]

To further address your request, this report focuses on DHS efforts to work with asset owners and operators[14] to incorporate and enhance resiliency, commensurate with DHS's increased emphasis on resiliency in the NIPP. Specifically, we assessed the extent to which DHS

- has taken action to incorporate resiliency into the programs it uses to work with asset owners and operators, and
- is positioned to disseminate information it gathers about resiliency practices to asset owners and operators within and across sectors.

To assess the extent to which DHS has taken action to incorporate resiliency into the programs it uses to work with asset owners and operators, we reviewed DHS policies, procedures, and documents on partnering and information sharing between the public and private sectors including the NIPP; sector-specific plans; and sector annual reports. We interviewed senior DHS officials responsible for planning, coordinating, and overseeing the national effort to reduce risk to CIKR to obtain information on DHS's efforts to work with CIKR partners, including asset owners and operators. Furthermore, we reviewed DHS documents on programs used to assess vulnerability and risk at CIKR facilities and the tools DHS uses to assess vulnerability to examine the extent to which, and in what context, the concept of resiliency was used as part of those assessments. Because it was out of the scope of our work, we did not assess the implementation or results of these assessments. In addition, we reviewed and analyzed DHS documents and reports resulting from these

[13] Based on guidance from DHS, the sector-specific plans were developed jointly by the SSAs in close collaboration with the SCCs, GCCs, and others, including state, local, and tribal CIKR partners with key interests or expertise appropriate to the sector. The plans for the original 17 sectors were officially released on May 21, 2007, after review and comment by the Homeland Security Council's Critical Infrastructure Protection Policy Coordination Committee which is responsible for coordinating the development and implementation of homeland security policies by multiple departments and agencies throughout the federal government, and coordinating those policies with state and local government. The SSP for the Critical Manufacturing Sector is under development and is scheduled for release in 2010 along with updated sector-specific plans for all other sectors.

[14] As defined in the 2009 NIPP, asset owners and operators are those entities responsible for day-to-day operation and investment in a particular asset or system.

vulnerability assessments. We selected 4 of 17 sectors—the chemical, commercial facilities, communications, and energy sectors—based on our analysis of sector-specific plans published in fiscal year 2007.[15] In making our selections, we focused on the extent to which the plans (1) discussed the concept of resiliency while considering key terms associated with resiliency—resilience, resilient, and continuity (business or operational continuity)[16] and (2) provided key information on various factors—including goals and objectives, measuring performance, and processes for prioritizing assets and assessing vulnerability—called for in DHS guidelines for developing these plans. We used our analysis to rank the sectors and conferred with various DHS officials familiar with the sector plans about the results of our analysis. Based on these discussions, we selected 2 of the highest and 2 of the lowest ranked sectors in terms of discussing resiliency concepts and providing key information.

We also used our selection methodology as the basis for interviewing representatives—owners and operators—of assets, also known as facilities, in two geographic locations. These facilities were (1) designated as a level 1 or 2 asset on the DHS critical asset list and (2) located in areas that had recently been affected by disasters (hurricanes in Texas and wildfires in California). We chose these locations to visit considering the type of disaster and geographic dispersion. During our site visits, we interviewed representatives of 15 individual assets, including representatives that worked on-site and in the corporate office, to determine the extent to which they receive guidance on resiliency from and partner with DHS. Among other things, we focused on the role of Protective Security Advisors (PSAs) who serve as liaisons between DHS and security stakeholders, to include asset owners and operators, in local communities. We also reviewed PSA program guidance and interviewed 10 of 93 PSAs to discuss their roles and responsibilities in partnering with asset owners and operators to incorporate resiliency practices and their knowledge of resiliency policies, practices, and techniques.[17] We selected these PSAs from a nonprobability sample based on a variety of factors including geographic location, the number of CIKR assets in a location,

[15] The scope of our review did not include the critical manufacturing sector (the 18th sector) because DHS had not developed its sector-specific plan at the time of our review.

[16] In commenting on our approach, DHS said this is a reasonable set of terms for our analysis.

[17] At the time of our review, DHS had deployed 93 PSAs nationwide.

and types and frequency of natural disasters in the region.[18] While the results of our interviews cannot be generalized to reflect the views of all asset owners and operators or PSAs nationwide, the information obtained provided us with the perspectives of various asset owners and operators and PSAs about critical infrastructure protection and resiliency. We also interviewed DHS officials about their plans for revising the various assessment programs and tools and compared the results of our work with The Standard for Program Management, which provides guidelines for successfully managing programs and projects.[19] We also compared the results of our efforts and DHS's PSA guidance with criteria in the Standards for Internal Control in the Federal Government[20] and the Standard for Program Management.[21]

To assess the extent to which DHS is positioned to disseminate information it gathers about resiliency practices with asset owners and operators within and across sectors, we reviewed DHS policies, procedures, and documents including the NIPP, sector-specific plans, and sector annual reports on CIKR information sharing with a particular focus on DHS's approach to information sharing on protective measures and resiliency practices and strategies with asset owners and operators. We interviewed DHS officials on their efforts to share information and facilitate the sharing of information on resiliency practices. In addition, we

[18] Nonprobability sampling is a method of sampling when nonstatistical judgment is used to select members of the sample, usually specific characteristics of the population as criteria. Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

[19] Project Management Institute, *The Standard for Program Management©* (Newtown Square, Pa: 2006).

[20] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD 00-21.3.1 (Washington, D.C.: November 1999). Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government.*

[21] Project Management Institute.

interviewed representatives of 15 assets in Texas and California about the mechanisms, policies, and practices DHS uses to facilitate the sharing of information related to resiliency, what resiliency-related practices associated with disasters they had identified, the extent to which they have implemented or are continuing to implement such practices into their daily operations, and whether they shared these best practices with DHS and other CIKR partners.

We conducted this performance audit from August 2008 through September 2010 in accordance with generally accepted government auditing standards.[22] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

Background

The Homeland Security Act, as well as other statutes, provide legal authority for both cross-sector and sector-specific protection and resiliency programs. For example, the purpose of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 is to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies,[23] and the Pandemic and All-Hazards Preparedness Act of 2006 addresses public health security and all-hazards preparedness and response.[24] Also, the Cyber Security Research and Development Act of 2002 authorized funding for the National Institute of Standards and Technology and the National Science Foundation to facilitate increased research and development for computer and network security and to support research fellowships and training.[25] CIKR protection issues are also covered under various

[22] As part of this work, we also issued a companion report in March 2010 on DHS's efforts to address resiliency. See GAO-10-296.

[23] Pub. L. No. 107-188, 116 Stat. 594 (2002).

[24] Pub. L. No. 107-188, 116 Stat. 594 (2002); Pub. L. No. 109-417, 120 Stat. 2831 (2006).

[25] Pub. L. No. 107-305, 116 Stat. 2367 (2002). Other statutes include the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007); the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064 (2002); the Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat. 597 (2001); the Energy Policy and Conservation Act, Pub. L. No. 94-163, 89 Stat. 871 (1975); the Critical Infrastructure Information Act, 6 U.S.C. §§ 131-34; and the Federal Information Security Management Act, 44 U.S.C. §§ 3541-49.

presidential directives, including HSPD-5 and HSPD-8.[26] HSPD-5 calls for coordination among all levels of government as well as between the government and the private sector for domestic incident management, and HSPD-8 establishes policies to strengthen national preparedness to prevent, detect, respond to, and recover from threatened domestic terrorist attacks and other emergencies.[27] These separate authorities and directives are tied together as part of the national approach for CIKR protection through the unifying framework established in HSPD-7.

The NIPP outlines the roles and responsibilities of DHS and its partners—including other federal agencies, state, local, territorial, and tribal governments, and private companies. Within the NIPP framework, DHS is responsible for leading and coordinating the overall national effort to enhance protection via 18 CIKR sectors. HSPD-7 and the NIPP assign responsibility for CIKR sectors to SSAs. As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of sector partners to protect 11 of the 18 CIKR sectors. The remaining sectors are coordinated by 8 other federal agencies. Table 1 lists the SSAs and their sectors.

[26] Homeland Security Presidential Directive Number 5 (Washington, D.C.: Feb. 28, 2003) and Homeland Security Presidential Directive Number 8 (Washington, D.C.: Dec. 17, 2003).

[27] Other CIKR-related presidential directives include HSPD-3, which addresses the Homeland Security Advisory System; HSPD-9, which discusses the defense of U.S. Agriculture and Food; HSPD-10, which addresses biodefense for the 21st Century; HSPD-19, which deals with combating terrorist use of explosives in the United States; HSPD-20, which addresses national continuity policy; and HSPD-22, which discusses domestic chemical defense.

Table 1: SSAs and CIKR Sectors

Sector-specific agency	Critical infrastructure and key resource sector
Departments of Agriculture[a] and Food and Drug Administration[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security	
• Office of Infrastructure Protection	Commercial Facilities Critical Manufacturing Emergency Services Nuclear Reactors, Materials, and Waste Dams Chemical Sectors
• Office of Cyber Security and Communications	Information Technology Communications Sectors
• Transportation Security Administration	Postal and Shipping
• Transportation Security Administration and U. S. Coast Guard[f]	Transportation Systems[g]
• Federal Protective Service[h]	Government Facilities[i]

Source: 2009 National Infrastructure Protection Plan.

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

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

[c]Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d]The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[e]The Water Sector includes drinking water and wastewater systems.

[f]The U.S. Coast Guard is the SSA for the maritime transportation mode within the Transportation System Sector.

[g]In accordance with HSPD-7, the Department of Transportation and the Department of Homeland Security are to collaborate on all matters relating to transportation security and transportation infrastructure protection.

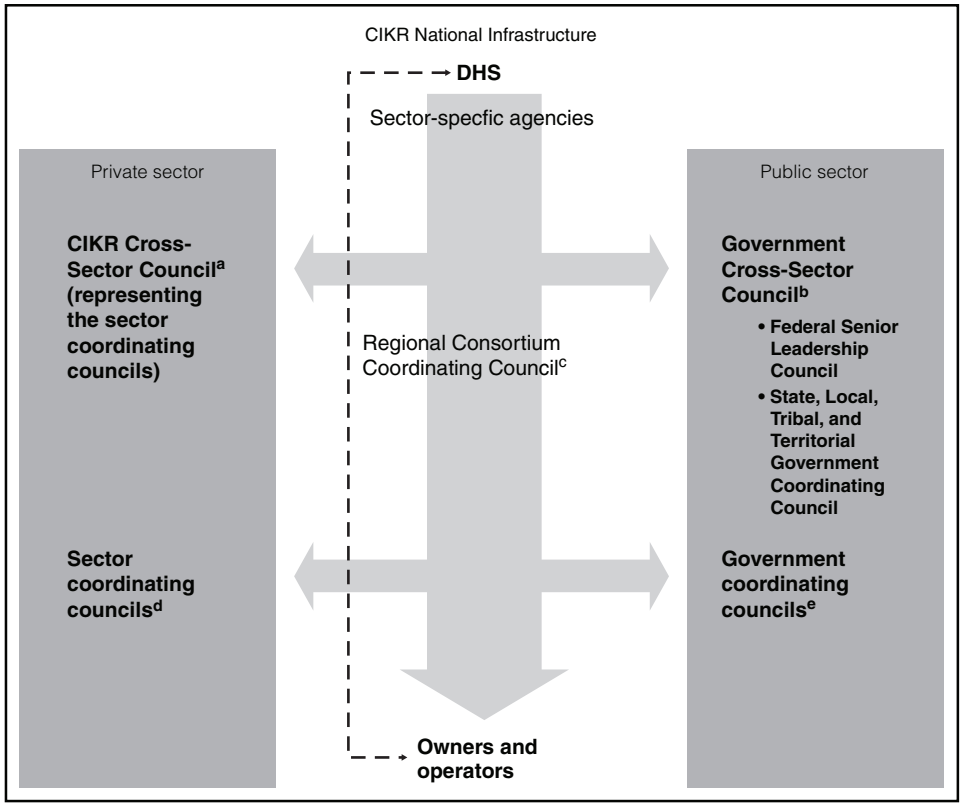
[h]As of October 2009, the Federal Protective Service transitioned out of Immigration and Customs Enforcement to the National Protection and Programs Directorate.

[i]The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

The DHS's Office of Infrastructure Protection (IP), located in the National Protection and Programs Directorate, is responsible for working with public- and private-sector CIKR partners and leads the coordinated national effort to mitigate risk to the nation's CIKR through the development and implementation of the CIKR protection program. Using a sector partnership model, IP's Partnership and Outreach Division (POD) works with owners and operators of the nation's CIKR to develop, facilitate, and sustain strategic relationships and information sharing, including the sharing of best practices. The POD also works with public and private partners to coordinate efforts to establish and operate various councils intended to protect CIKR and provide CIKR functions to strengthen incident response. These councils include the aforementioned SCCs, which coordinate sectorwide CIKR activities and initiatives among private sector owners, operators, and trade associations in each of the 18 sectors, and the GCCs that represent federal, state, and local government and tribal interests to support the effort of SCCs to develop collaborative strategies for CIKR protection for each of the 18 sectors. The partnership model also includes various cross-sector councils, including the CIKR Cross-Sector Council, which addresses cross-sector issues and interdependencies among SCCs; the NIPP Federal Senior Leadership Council, which focuses on enhanced communication and coordination between and among federal departments and agencies responsible for implementing the NIPP and HSPD-7; and the State, Local, Tribal, and Territorial Government Coordinating Council, which promotes coordination across state and local jurisdictions. The model also includes a Regional Consortium Coordinating Council, which bring together representatives of regional partnerships, groupings, and governance bodies to foster coordination among CIKR partners within and across geographical areas and sectors.

Figure 1 illustrates the sector partnership model and the interrelationships among the various councils, sectors, and asset owners and operators.

Figure 1: The CIKR Sector Partnership Model and the Interrelationships among CIKR Councils, Sectors, and Asset Owners and Operators



Source: GAO analysis of the 2009 National Infrastructure Protection Plan.

[a]Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of all SCCs.

[b]Cross-sector issues and interdependencies between the GCCs are to be addressed through the Government Cross-Sector Council, which comprises two subcouncils—the NIPP Federal Senior Leadership Council and the State, Local, Tribal, and Territorial Government Coordinating Council. The objective of the NIPP Federal Senior Leadership Council is to facilitate enhanced communications and coordination between and among federal departments and agencies with a role in implementing the NIPP and HSPD-7. The State, Local, Tribal, and Territorial Government Coordinating Council serves as a forum to ensure that state, local, and tribal homeland security partners are fully integrated as active participants in national CIKR protection efforts and to provide an organizational structure to coordinate across jurisdictions on state and local government-level CIKR protection guidance, strategies, and programs.

[c]The Regional Consortium Coordinating Council brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among CIKR partners within and across geographical areas and sectors.

[d]The SCCs are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership varies from sector to sector, reflecting the unique composition of each sector; however, membership is to be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector.

[e]The GCCs comprise representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector.

IP's Protective Security Coordination Division (PSCD) also operates the Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists, called PSAs, to local communities throughout the country. Established in 2004, the program has 93 PSAs serving in 74 districts in 50 states and Puerto Rico, with deployment locations based on population density and major concentrations of CIKR throughout the United States. PSAs lead IP's efforts in these locations and act as the link between state, local, tribal, and territorial organizations and DHS infrastructure mission partners. PSAs are to assist with ongoing state and local CIKR security efforts by establishing and maintaining relationships with state Homeland Security Advisors, State Critical Infrastructure Protection stakeholders, and other state, local, tribal, territorial and private-sector organizations. PSAs are to support the development of the national risk picture by conducting vulnerability and security assessments to identify security gaps and potential vulnerabilities in the nation's most critical infrastructures. PSAs also are to share vulnerability information and protective measure suggestions with local partners and asset owners and operators. In addition, PSAs are to coordinate training for private-and public-sector officials in the communities in which they are located; support incident management; and serve as a channel of communication for state, local, tribal, and territorial officials and asset owners and operators seeking to communicate with DHS.

Critical Infrastructure and the Concept of Resiliency

The concept of resiliency has gained particular importance and application in a number of areas of federal CIKR planning. Both Congress and executive branch agencies have addressed resilience in relation to the importance of the recovery of the nation's critical infrastructure from damage. In March 2010 we reported that, since 2006, various organizations, including DHS, have emphasized the importance of resiliency and the concepts associated with resiliency—e.g., recovery and reconstitution and continuity of operations—have evolved over the years.[28] In February 2010, DHS issued its Quadrennial Homeland Security Review (QHSR) Report, which cited resilience as one of three key concepts that are essential to, and form the foundation for, a comprehensive approach to homeland

[28] GAO-10-296.

security.[29] The report defines five missions, including ensuring resiliency to disasters.[30] Each mission is accompanied by goals and objectives. Regarding ensuring resiliency to disasters, the QHSR report states that:

"Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as deliberate attacks, will occur. The challenge is to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises. Our vision is a Nation that understands the hazards and risks we face; is prepared for disasters; can withstand the disruptions disasters may cause; can sustain social trust, economic, and other functions under adverse conditions; can manage itself effectively during a crisis; can recover quickly and effectively; and can adapt to conditions that have changed as a result of the event."

The report also articulates that one of the goals for this mission is to "Rapidly Recover." The two objectives associated with this goal are to (1) enhance recovery capabilities: establish and maintain nationwide capabilities for recovery from major disasters and (2) ensure continuity of essential services and functions: improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.

[29] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010). The report discusses resilience in the context of fostering individual, community, and system robustness, adaptability, and capacity for rapid recovery. The other two concepts are security and customs and exchange. The QHSR report was issued pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 2401, 121 Stat. 266, 543-46 (2007). According to DHS, the QHSR is to outline the strategic framework that guides the activities of participants in homeland security to a common end. According to DHS, the QHSR has led directly to an examination of DHS's activities from the bottom up in order to make recommendations regarding programs, assets, and capabilities, as well as policies, authorities, and organizational effectiveness in its fiscal year 2012 budget submission.

[30] The other four missions are preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; and safeguarding and securing cyberspace.

DHS Efforts to Incorporate Resiliency into Programs Used to Work with Asset Owners and Operators Is Evolving but Program Management Could Be Strengthened

Consistent with recent changes to the NIPP, DHS has begun to increase its emphasis on resiliency in the various programs it uses to assess vulnerability and risk at and among CIKR facilities so that it can help asset owners and operators identify resiliency characteristics of their facilities and provide suggested actions, called options for consideration, to help them mitigate gaps that have been identified. However, DHS has not developed an approach to measure owners' and operators' actions to address resiliency gaps identified as a result of these assessments. DHS has also begun to train PSAs about resiliency and how it applies to asset owners and operators, but it has not updated guidance that discusses PSAs' roles and responsibilities to explicitly include resiliency and resiliency strategies.

DHS Has Increased Emphasis on Resiliency in Programs, but Has Not Developed an Approach to Measure Performance

In March 2010 we reported that DHS has increased its emphasis on resiliency in the 2009 NIPP by, among other things, generally pairing it with the concept of protection. We further stated that DHS has encouraged SSAs to emphasize resiliency in guidance provided to them in updating their sector-specific plans.[31] Consistent with these efforts, DHS has also taken action to develop or enhance the programs it uses to work with asset owners and operators to bring a stronger focus to resiliency.

The Regional Resiliency Assessment Program (RRAP) and the Mini-Resiliency Assessment Program (Mini-RAP)

In 2009 DHS developed the RRAP to assess vulnerability and risk associated with resiliency.[32] The RRAP is an analysis of groups of related infrastructure, regions, and systems in major metropolitan areas. The RRAP evaluates CIKR on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to

[31] For example, the DHS guidance for developing the 2010 sector-specific plans includes a resiliency term in many places where there is a reference to "protection" or "protection programs" and provides instructions for where—and at times, how—resiliency is to be incorporated into the 2010 plans. We did not examine the 2010 sector-specific plans to determine the extent to which the SSAs adhered to DHS's SSP guidance because these plans were not complete at the time of our review. Although representatives of 17 of 18 SSAs told us they believe that they have already included the concept of resiliency in their existing sector-specific plans, they said that they intend to further incorporate resiliency into their 2010 plans where appropriate based on the characteristics of their sectors and their understanding of DHS guidance.

[32]The RRAP was piloted under five projects—the New York Bridges; the New Jersey Turnpike Exit 14 Chemical Corridor; the Raleigh/Durham Research Triangle Park; the Tennessee Valley Authority; and the Chicago Financial District.

identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps. In conducting the RRAP, DHS does an analysis of a region's CIKR and protection and prevention capabilities and focuses on (1) integrating vulnerability and capability assessments and infrastructure protection planning efforts; (2) identifying security gaps and corresponding options for considerations to improve prevention, protection, and resiliency; (3) analyzing system recovery capabilities and providing options to secure operability during long-term recovery; and (4) assessing state and regional resiliency, mutual aid, coordination, and interoperable communication capabilities. RRAP assessments are to be conducted by DHS officials, including PSAs, in collaboration with SSAs: other federal officials; state, local, tribal, and territorial officials; and the private sector depending upon the sectors and facilities selected as well as a resiliency subject matter expert(s) deployed by the state's homeland security agency. The results of the RRAP are to be used to enhance the overall security posture of the facilities, surrounding communities, and the geographic region covered by the project and are shared with the state. According to DHS officials, the results of specific asset-level assessments conducted as part of the RRAP are made available to asset owners and operators and other partners (as appropriate), but the final analysis and report is delivered to the state where the RRAP was conducted.

One of the assessment tools DHS developed for the RRAP analysis is a "resiliency assessment builder," which contains a series of questions designed to help officials identify resiliency issues associated with facilities included in the RRAP. The resiliency assessment builder, among other things, focuses on:

- the impact of loss associated with the facility, including any national security, sociopolitical, and economic impacts;
- interdependencies between the facility under review and other infrastructure—such as electrical power or natural gas suppliers, water, and supply chain systems—that if disrupted, could cause deterioration or cessation of facility operations;
- the impact of the loss of significant assets—such as an electrical substation to provide power or a rail spur to transport supplies—critical to the operation of the facility and backup systems available to maintain operations if losses occur; and
- specific vulnerabilities, unusual conditions, threats, or events—such as hurricanes, transportation chokepoints, or hazardous materials

issues—that could disrupt operations and whether the facility is prepared to address the situation via specific capabilities or an action plan.

Senior IP officials told us that they believe the RRAP has been successful in helping DHS understand resiliency in the context of interdependencies among individual assets. For example, while the focus of the Tennessee Valley Authority RRAP was energy sector sites and resources, DHS and its partners examined sites and resources in those sectors, like water and dams, which appeared to be obvious interdependencies. However, they also found that they needed to examine sites and resources in those sectors that appeared less obvious but were interdependent because they were intricately connected to the Tennessee Valley Authority operations, like sites and resources in the transportation sector. Also, in fiscal year 2010, DHS started an RRAP in Atlanta that focused primarily on commercial facilities. DHS's related vulnerability assessment of sites (see the discussion below for additional details of these assessments) and resources associated with the water sector in Atlanta showed that an accident or attack involving one component of the water sector could disrupt the operations of sites or resources of other sectors in the geographic area covered by the RRAP. By discovering this vulnerability, and taking steps to address it, asset owners and operators in various sectors that were provided this information were better positioned to be able to work together to mitigate this potential problem. Senior IP officials said that the overall RRAP effort was piloted in five projects, but they no longer consider it a pilot program. They added that they plan to conduct five other RRAPs in 2010 in addition to the one already started in Atlanta. They further stated that because the program focuses only on areas with a high density of critical assets, they plan to develop a new "mini-RAP." According to these officials, the mini-RAP is intended to provide assessments similar to those provided during an RRAP (but on a reduced scale) to groups of related infrastructure or assets that are not selected to receive an RRAP. An IP official stated that he anticipates that the mini-RAP, which is under development, will be finalized in October 2010.

Site Assistance Visits (SAVs)

DHS is also revising another vulnerability assessment called the SAV to foster greater emphasis on resiliency at individual CIKR sites. The SAV, which is a facility-specific "inside-the-fence" vulnerability assessment conducted at the request of asset owners and operators, is intended to identify security gaps and provide options for consideration to mitigate these identified gaps. SAVs are conducted at individual facilities or as part of an RRAP and are conducted by IP assessment teams in coordination

with PSAs, SSAs, state and local government organizations (including law enforcement and emergency management officials), asset owners and operators, and the National Guard, which is engaged as part of a joint initiative between DHS and the National Guard Bureau. The National Guard provides teams of subject matter experts experienced in conducting vulnerability assessments. The private sector asset owners and operators that volunteer for the SAV are the primary recipient of the SAV analysis, which produces options for consideration to increase their ability to detect and prevent terrorist attacks. In addition, it provides mitigating options that address the identified vulnerabilities of the facility. The SAV is developed using a questionnaire that focuses on various aspects of the security of a facility, such as vulnerabilities associated with access to facility air handling systems; physical security; and the ability to deter or withstand a blast or explosion. Our review of the SAV questionnaire showed that it focuses primarily on vulnerability issues related to the protection of the facility. The SAV questionnaire also contains some questions that focus on resiliency issues because it asks questions about backup systems or contingencies for key systems, such as electrical power, transportation, natural gas, water, and telecommunications systems. Officials with IP's PSCD said that they are working with IP's Field Operations Branch to update the SAV to include more questions intended to capture the resiliency of a facility, especially since the SAV is used during the RRAP. They said that the effort is ongoing and, as of June 8, 2010, DHS had developed a time line showing the revised SAV is to be introduced in October or November 2010.

Enhanced Critical Infrastructure Protection (ECIP) Security Survey

DHS is also revising its ECIP security survey to further focus on resiliency at individual facilities.[33] Under the ECIP survey, PSAs meet with facility owners and operators in order to provide awareness of the many programs, assessments, and training opportunities available to the private sector; educate owners and operators on security; and promote communication and information sharing among asset owners and operators, DHS, and state governments. ECIP visits are also used to conduct security surveys using the ECIP security survey, a Web-based tool developed by DHS to collect, process, and analyze vulnerability and protective measures information during the course of a survey. The ECIP security survey is also used to develop metrics; conduct sector-by-sector

[33]During our review, this assessment program was referred to as the ECIP security assessment. However, in its technical comments, DHS indicated that the program is now referred to as the ECIP security survey.

and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; establish sector baseline security survey scores; and track progress toward improving CIKR security through activities, programs, outreach, and training. Our review of the ECIP security survey showed that the original version of the survey made references to resiliency-related concepts—business continuity plans and continuity of operations. The newest version of the survey, published in June 2009, contains additional references to resiliency and resiliency-related concepts, including identifying whether or not a facility has backup plans for key resources such as electrical power, natural gas, telecommunications, and information technology systems. It is also used to identify key dependencies critical to the operation of the facility, such as water and wastewater, and to state whether backup plans exist for service or access to these dependencies in the event of an interruption. Further, senior IP officials told us that in addition to the updates on resiliency in the latest version of the ECIP security survey, they plan to incorporate 22 additional questions to a subsequent update of the survey that will focus on determining the level of resiliency of a facility. According to these officials, DHS also intends to use the updated survey to develop a resiliency "dashboard" for CIKR owners and operators that is intended to provide them a computerized tool that shows how the resiliency of their facility compares with other similar facilities (see the discussion below for a more detailed discussion of DHS's ECIP dashboard). A DHS document on revisions to the SAV showed that the revised ECIP security survey is to be introduced at the same time as the revised SAV (October or November 2010) so that data collection associated with each remains compatible. DHS's current projected release of the updated ECIP security survey is planned for October 2010.

Program Management Could Be Improved by Measuring Efforts to Mitigate Resiliency Gaps Identified during Vulnerability Assessments

DHS intends to take further actions to enhance the programs and tools it uses to work with asset owners and operators when assessing resiliency, but it has not developed an approach to measure its effectiveness in working with asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during the various vulnerability assessments. According to the NIPP, the use of performance measures is a critical step in the NIPP risk management process to enable DHS and the SSAs to objectively and quantitatively assess improvement in CIKR protection and resiliency at the sector and national levels. The NIPP states that while the results of risk analyses help sectors set priorities, performance metrics allow NIPP partners to track progress against these priorities and provide a basis for DHS and the SSAs to establish accountability, document actual performance, facilitate diagnoses, promote effective management, and provide a feedback mechanism to

decision makers. Consistent with the NIPP, senior DHS officials told us that they have recently begun to measure the rate of asset owner and operator implementation of protective measures following the conduct of the ECIP security survey. Specifically, in a June 2010 memorandum to the Assistant Secretary for NPPD, the Acting Director of PSCD stated that 234 (49 percent) of 437 sites where the ECIP security survey had been conducted implemented protective measures during the 180-day period following the conduct of the ECIP survey. The Acting Director reported that the 234 sites made a total of 497 improvements across the various categories covered by the ECIP security survey, including information sharing, security management, security force, physical security, and dependencies while 239 sites reported no improvements during the period. The Acting Director stated that the metrics were the first that were produced demonstrating the impact of the ECIP program, but noted that PSCD is reexamining the collection process to determine whether additional details should be gathered during the update to the ECIP security survey planned for October 2010. However, because DHS has not completed its efforts to include resiliency material as part of its vulnerability assessment programs, it does not currently have performance metrics of resiliency measures taken by asset owners and operators.

Moving forward, as DHS's efforts to emphasize resiliency evolve through the introduction of new or revised assessment programs and tools, it has the opportunity to consider including additional metrics of resiliency measures adopted at the facilities it assesses for vulnerability and risk, particularly as it revises the ECIP security survey and develops the resiliency dashboard. Moreover, DHS could consider developing similar metrics for the SAV at individual facilities and the RRAP and mini-RAP in the areas covered by RRAPs and mini-RAPs. By doing so, DHS could be able to demonstrate its effectiveness in promoting resiliency among the asset owners and operators it works with and would have a basis for analyzing performance gaps. Regarding the latter, DHS managers would have a valuable tool to help them assess where problems might be occurring or alternatively provide insights into the tools used to assess vulnerability and risk and whether they were focusing on the correct elements of resiliency at individual facilities or groups of facilities.

DHS Has Made Training on Resiliency Available to PSAs, but Guidelines on PSA Roles and Responsibilities Do Not Reflect DHS's Growing Emphasis on Resiliency

DHS uses PSAs to provide assistance to asset owners and operators on CIKR protection strategies. Although DHS had begun to train PSAs about resiliency and how it applies to the owners and operators they interact with, DHS has not updated PSAs' guidance that outlines their roles and responsibilities to reflect DHS's growing emphasis on resiliency. In April 2010, DHS provided a 1-hour training course called "An Introduction to Resilience" to all PSAs at a conference in Washington, D.C. The training was designed to define resilience; present resilience concepts, including information on how resilience is tied to risk analysis and its link to infrastructure dependencies and interdependencies; discuss how resilience applies to PSAs, including a discussion of the aforementioned updates to programs and tools used to do vulnerability assessments; and explain how DHS's focus on resilience can benefit asset owners and operators. According to the Acting Deputy Director of PSCD, PSCD is expected to deliver the training to PSAs again during regional conferences to foster further discussions about resiliency and to give PSAs an additional opportunity to ask questions about the training they received in April 2010.[34]

Although DHS's training discusses how resiliency applies to PSAs and how it can benefit asset owners and operators, DHS has not updated guidance that discusses PSA roles and responsibilities related to resiliency. The guidance DHS has provided to PSAs on certain key job tasks, issued in 2008, includes discussions about how PSAs are to (1) implement their role and responsibilities during a disaster; (2) conduct vulnerability assessments; and (3) establish or enhance existing strong relationships between asset owners and operators and DHS, federal, state, and local law enforcement personnel. However, the guidance does not articulate the role of PSAs with regard to resiliency issues, or how PSAs are to promote resiliency strategies and practices to asset owners and operators. For example, our review of DHS's engagement guidance for PSAs showed that the guidance does not explicitly discuss resiliency; rather, it focuses primarily on protection. Specifically, the executive summary of the guidance states that one of the key infrastructure protection roles for DHS in fiscal year 2008 was to form partnerships with the owners and operators of the nation's identified high-priority CIKR, known as level 1 and level 2

[34] According to DHS officials, DHS also has a professional training program to prepare and help PSAs carry out their roles and responsibilities. The program includes professional certification courses, such as those required to become a board Certified Protection Professional. According to DHS, this certification designates individuals who have demonstrated competency in all areas constituting security management.

assets and systems. The guidance describes particular PSA responsibilities with regard to partnerships, including (1) identifying protective measures currently in place at these facilities and tracking the implementation of any new measures into the future; (2) informing owners and operators of the importance of their facilities in light of the ever-present threat of terrorism; and (3) establishing or enhancing existing relationships between owners and operators, DHS, and federal, state, and local law enforcement personnel to provide increased situational awareness regarding potential threats, knowledge of the current security posture at each facility, and a federal resource to asset owners and operators. There is one reference to a resiliency-related concept in an appendix where DHS indicated that the criteria to identify level 2 assets in the Information Technology sector should be "those assets that provide incident management capabilities, specifically, sites needed for rapid restoration or continuity of operations."

PSA program officials said that they are currently developing guidelines on a number of issues as DHS transitions from a CIKR program heavily focused on protection to one that incorporates and promotes resiliency. They said that PSAs do not currently have roles and responsibilities specific to "resiliency" because resiliency is a concept that has only recently gained significant and specific attention. They added that PSA roles and responsibilities, while not specifically mentioning resiliency, include component topics that comprise or otherwise contribute to resiliency as it is now defined. Nonetheless, the Acting Deputy Director of IP's PSCD said that he envisions updating PSA guidance to incorporate resiliency concepts and that he intends to outline his plan for doing so in October 2010 as part of IP's program planning process. However, he was not specific about the changes he plans to make to address resiliency concepts or whether the PSA's roles and responsibilities related to resiliency would be articulated. According to standards for internal control in the federal government, management is responsible for developing and documenting the detailed policies and procedures to ensure that they are an integral part of operations.[35] By updating PSA guidance that discusses the role PSAs play in assisting asset owners and operators, including how PSAs can work with them to mitigate vulnerabilities and strengthen their security, PSA program officials would be better positioned to help asset owners and operators have the tools they need to develop resilience strategies. This would be consistent with

[35] GAO/AIMD 00-21.3.1.

DHS efforts to train PSAs about resiliency and how it affects asset owners and operators. Updating PSA guidelines to address resiliency issues would also be consistent with DHS's efforts to treat resiliency on an equal footing with protection, and would comport with DHS guidance that calls for SSAs to enhance their discussion of resiliency and resiliency strategies in SSPs.

DHS Could Better Position Itself to Disseminate Information about Resiliency Practices with Asset Owners and Operators within and across Sectors

DHS's efforts to emphasize resiliency in the programs and tools it uses to work with asset owners and operators also creates an opportunity for DHS to better position itself to disseminate information about resiliency practices to asset owners and operators within and across sectors. Currently, DHS shares information on vulnerabilities and protective measures on a case-by-case basis. However, while it is uniquely positioned and has considered disseminating information about resiliency practices, DHS faces barriers in doing so and has not developed an approach for sharing this information more broadly, across sectors.

DHS Shares Information on Vulnerabilities and Protective Measures on a Case-by-Case Basis

According to the NIPP, its effective implementation is predicated on active participation by government and private-sector partners in meaningful, multidirectional information sharing. The NIPP states that when asset owners and operators are provided with a comprehensive picture of threats or hazards to CIKR and participate in ongoing multidirectional information flow, their ability to assess risks, make prudent security investments, and develop appropriate resiliency strategies is substantially enhanced. Similarly, according to the NIPP, when the government is provided with an understanding of private-sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination accordingly. Consistent with the NIPP, DHS shares information on vulnerabilities and potential protective measures with asset owners and operators after it has collected and analyzed information during SAVs and ECIP security surveys performed at their individual facilities. This information includes vulnerabilities DHS has identified, and corresponding steps these owners and operators can take to mitigate these vulnerabilities, including options for consideration, which are suggestions presented to owners and operators to help them resolve vulnerabilities identified during DHS's assessments. For example, DHS issues SAV reports to owners and operators that, among other things, identify vulnerabilities; help them identify their security posture; provide options for consideration to increase their ability to detect and prevent terrorist attacks; and enhance their ability to mitigate vulnerabilities. Regarding the

ECIP security survey, DHS provides owners and operators an ECIP "dashboard" which shows the results for each component of the survey for a facility using an index, called the Protective Measures Index (PMI), which are scores DHS prepares for the facility and individual components that can be compared to other similar facilities' scores.[36] SAV reports and the ECIP dashboard generally focus on similar protection issues, such as facility or physical security, security personnel, and access control. The SAV reports and the ECIP dashboard discuss some continuity of operations issues that could be considered resiliency related. For example, the ECIP dashboard contains PMIs focused on whether the facility has a continuity plan and conducts continuity exercises, while the SAV report discusses whether the facility would be able to operate if resources such as electricity, water, or natural gas were not available. As discussed earlier, DHS is currently updating the SAV to include, among other things, an assessment of resiliency characteristics and gaps, and is taking action to develop a resiliency dashboard similar to that used under the ECIP security survey.

Senior IP officials also stated that they share information on steps owners and operators can take to protect their facilities via Common Vulnerabilities, Potential Indicators, and Protective Measures (CV/PI/PM) reports. DHS develops and disseminates these reports to various stakeholders, generally on a need-to-know basis, including specific owners and operators, such as those that have been included in assessments by PSAs; law enforcement officials, emergency responders, and state homeland security officials; and others who request access to the reports. These reports, which focus on vulnerabilities and security measures associated with terrorist attacks, are intended to provide information on potential vulnerabilities and specific protective measures that various

[36] The PMI is designed to (1) draw attention to components that are below or above the average for similar facilities and may deserve additional study and (2) show how a PMI can increase as protective measures are added, such as installing additional closed-circuit televisions along the street side of a facility to identify suspicious vehicles.

stakeholders can implement to increase their security posture.[37] According to DHS, these reports are developed based on DHS's experiences and observations gathered from a range of security-related vulnerability assessments, including SAVs, performed at infrastructures over time, such as the chemical and commercial facilities sectors and subsectors and asset types within those sectors, such as the chemical hazardous storage industry or the restaurant industry, respectively. For example, like other CV/PI/PM reports, DHS's report on the restaurant industry gives a brief overview of the industry; potential indicators of terrorist activity; common vulnerabilities; and protective measures. Common vulnerabilities include unrestricted public access and open access to food; potential indicators of terrorist activity include arson, small arms attack, persons wearing unusually bulky clothing to conceal explosives, and unattended packages; and protective measures include developing a comprehensive security plan to prepare for and respond to food tampering and providing appropriate signage to restrict access to nonpublic areas. The CV/PI/PM reports discuss aspects of resiliency such as infrastructure interdependencies and incident response, but they do not discuss other aspects of resiliency. For example, the report on restaurants discusses protective measures including providing security and backup for critical utility services, such as power or water—efforts that may also enhance the resiliency of restaurants. Moving forward, as its efforts to emphasize resiliency evolve, DHS could consider including other aspects of resiliency in the CV/PI/PM reports.

[37] DHS also provides more detailed industry-specific reports that address common vulnerability, potential indicators of terrorist activity, and protective measures. For example, an October 5, 2007, common vulnerability report on the petroleum extraction industry in the energy sector discusses specific threats to these facilities and the consequences of an event—as well as potential vulnerabilities—that apply to the petroleum extraction industry. To illustrate vulnerabilities, the report cited particular incidents, such as a rupture at an oil platform 6 miles off the coast of Santa Barbara, California, in 1969 that, according to DHS, resulted in the release of 200,000 gallons of crude oil and an 800-square-mile oil slick that marred 35 miles of coastline. The paper also discusses facility vulnerabilities and interdependent vulnerabilities that could affect the condition or functionality of the facility.

DHS Is Uniquely Positioned to Disseminate Information about Resiliency Practices but Faces Barriers

Senior IP officials told us that they have considered ways to disseminate information that DHS currently collects or plans to collect with regard to resiliency. However, they have not explored the feasibility of developing an approach for doing so. Senior IP officials explained that given the voluntary nature of the CIKR partnership, DHS should not be viewed as identifying or promoting practices, particularly best practices, which could be construed to be standards or requirements. They said that DHS goes to great lengths to provide assurance to owners and operators that the information gathered during assessments will not be provided to regulators. They also stated that they provide owners and operators assurance that they will not share proprietary information with competitors. For example, certain information that they collect is protected under the Protected Critical Infrastructure Information (PCII) program, which institutes a means for the voluntary sharing of certain private sector, state, and local CIKR information with the federal government while providing assurance that the information will be exempt from disclosure under the Freedom of Information Act, among other things, and will be properly safeguarded.[38] DHS has established a PCII program office, which among other things, is responsible for validating information provided by CIKR partners as PCII, and developing protocols to access and safeguard information that is deemed PCII.

IP senior officials further explained that DHS relies on its private-sector partners to develop and share information on practices they use to enhance their protection and resilience. They said that the practices shared by sector partners, including best practices, are largely identified and developed by the private sector, at times with the support of its partners in government such as the SSAs. DHS facilitates this process by making various mechanisms available for information sharing, including information they deem to be best practices. For example, according to senior IP officials, DHS's Homeland Security Information Network-Critical Sectors (HSIN-CS) was designed to provide each sector a portal to post useful or important information, such as activities or concepts that private-sector partners discern to be best practices on protection and

[38] The PCII program was established under the Critical Infrastructure Information (CII) Act of 2002. 6 U.S.C. §§ 131-34.

resiliency topics.[39] They also said that one factor to consider is that resiliency can mean different things to different sectors, as measures or strategies that are applicable or inherent to one sector may not be applicable to another given the unique characteristics of each sector. For example, the energy sector, which includes oil refineries, is inherently different than the government facilities sector, which includes government office buildings. In our March 2010 report on DHS's increased emphasis on resilience in the NIPP, we reported that DHS officials told us that the balance between protection and resiliency is unique to each sector and the extent to which any one sector increases the emphasis on resiliency in its sector-specific plans will depend on the nature of the sector and the risks to its CIKR.[40] Further, the Branch Chief of IP's Office of Information Coordination and Analysis Office explained that differences in corporate cultures across the spectrum of companies could be a barrier to widely disseminating information on resiliency practices because it is often challenging to translate information, such as what constitutes a success or failure, from one company to another. He further stated that differences in the regulatory structures affecting different industries may be a factor that could limit the extent to which certain types of information could be disseminated.

We recognize that DHS faces barriers to sharing information it gathers on resiliency practices within and among sectors. However, as the primary federal agency responsible for coordinating and enhancing the protection and resiliency of critical infrastructure across the spectrum of CIKR sectors, DHS is uniquely positioned to disseminate this information which would be consistent with the NIPP's emphasis on information sharing. By working to explore ways to address any challenges or barriers to sharing resiliency information, DHS could build upon the partnering and information-sharing arrangements that CIKR owners and operators use in their own communities. For example, our work at CIKR assets along the Gulf Coast in Texas and in southern California showed that asset owners and operators viewed resiliency as critical to their facilities because it is in their best interests to either keep a facility operating during and after an

[39] The HSIN-CIS portal is restricted, and provides authorized private-sector partners the capability to share information with other partners by posting/uploading information to their portal, particularly For Official Use Only or Sensitive but Unclassified documents on sector-specific practices, or on the master HSIN-CS portal, as deemed appropriate by each sector.

[40] GAO-10-296.

event, or rebound as quickly as possible following an event. They said that they rely on a variety of sources for information to enhance their ability to be more resilient if a catastrophic event occurs, including information-sharing or partnering arrangements within and among CIKR partners and their local communities. Each of the 15 owners and operators we contacted in Texas and California said that they have partnering relationships with their sector coordinating councils, local/state government, law enforcement, emergency management, or mutual aid organizations. Furthermore, 14 of the 15 said that they work with these organizations to share information, including best practices and lessons learned, from recent disasters. Among the owners and operators we contacted:

- Representatives of one facility said that following a recent event, their company shared lessons learned with the local mutual aid association and various trade associations. These officials said that they also share best practices within the industry and across their facilities in other locations on an ongoing basis and that the company is currently organizing a committee made up of security staff from each facility within the organization whose primary responsibility is expected to be the sharing of best practices.

- Officials representing another facility told us that following an event or a drill, they critique the event and their response to garner any lessons learned or best practices. They said that they share information with the local fire department and a regional trade association. These officials stated that they will share information with other trade association members if they believe that it would be beneficial to others, but will not discuss proprietary information.

- Officials representing a different facility said that, following a hurricane in the same area, the company's managers from various facilities met to share lessons learned and adopted best practices from other facilities within the same company and with external partners, including a mutual aid organization and local emergency responders. They said that they also have learned from the experiences of others—after an explosion at a similar company's facility, they became aware that the other company had located its administration building too close to the company's operations, thereby jeopardizing employee safety.

By developing an approach for disseminating information it gathers or intends to gather with regard to resiliency, DHS would then be in a

position to reach a broader audience across sectors or in different geographic locations. Senior IP officials said that they agree that disseminating information on resiliency practices broadly across the CIKR community would be a worthwhile exercise, but questioned whether they would be the right organization within DHS to develop an approach for sharing resiliency information. They said that IP does not currently have the resources to perform this function and suggested that an organization like the Federal Emergency Management Agency (FEMA) might be more appropriate for sharing information on resiliency because it already has mechanisms in place to share information on practices organizations can adopt to deal with all-hazards events, including terrorism. For example, FEMA manages DHS's Lessons Learned Information Sharing portal, called LLIS.gov, which is a national online network of lessons learned and best practices designed to help emergency response providers and homeland security officials prevent, prepare for, and respond to all hazards, including terrorism. According to FEMA officials, LLIS.gov contains information on critical infrastructure protection and resiliency and system users, such as state and local government officials, are encouraged to submit content which is then vetted and validated by subject matter experts before being posted to the system. FEMA officials explained that FEMA does not actively collect information from system users, but encourages them to submit documents for review and possible inclusion into LLIS.gov. According to FEMA, access to LLIS.gov is restricted to members that request access to the system, particularly emergency response providers and homeland security officials. In March 2010, FEMA's Outreach and Partnerships Coordinator for Lessons Learned Information Sharing told us that LLIS.gov had about 55,000 members, of which approximately 89 percent were representatives of state and local government; about 6 percent were representatives of private-sector organizations; and about 5 percent were representatives of the federal government.

Regardless of which DHS organization would be responsible for disseminating information on resiliency practices, we recognize that DHS will face challenges in addressing any barriers it believes could hinder its ability to disseminate resiliency information. As part of this effort, DHS would have to determine what resiliency information it is collecting or plans to collect that might be most appropriate to share and what safeguards would be needed to protect against the disclosure of proprietary information within the confines of the voluntary nature of the CIKR partnership. Also, in doing so, DHS could consider some of the following questions:

- What additional actions, if any, would DHS need to take to convey that the information is being gathered within the voluntary framework of the CIKR partnership?

- To what extent does DHS need to take additional actions, if any, to provide assurance that the information being disseminated is nonregulatory and nonbinding on the owners and operators that access it?

- What additional mechanisms, if any, does DHS need to establish to provide assurance that reinforces the PCII process and how can resiliency practices information be presented to avoid disclosures of information that is PCII security sensitive or proprietary in nature?

- What mechanism or information system is most suitable for disseminating resiliency practices information, and which DHS component would be responsible for managing this mechanism or system?

- What approach should DHS take to review the information before it is disseminated to ensure that resiliency practices identified by DHS at one facility or in one sector are valid and viable, and applicable across facilities and sectors? [41]

- What additional resources and at what additional cost, if any, would DHS need to devote to gathering and broadly disseminating information about resiliency practices across facilities and sectors?

- What actions can DHS take to measure the extent to which asset owners and operators are using resiliency information provided by DHS, and how can DHS use this information to make improvements, if needed?

By determining the feasibility of overcoming barriers and developing an approach for disseminating resiliency information, DHS could better position itself to help asset owners and operators consider and adopt

[41] According to DHS, one factor to consider, when considering resiliency in any context, is that there are trade-offs when owners and operators make decisions to improve security and resiliency. For example, an owner and operator could decide to store additional quantities of a hazardous material necessary for emergency operation. The hazardous material would improve the resiliency of the facility but the storage of the material on site increases the security risk and vulnerability.

resiliency strategies, and provide them with information on potential security investments, based on the practices and experiences of their peers both within and across sectors.

Conclusions

In the wake of concerns by stakeholders, including members of Congress, academia, and the private sector that DHS was placing emphasis on protection rather than resilience, DHS has increased its emphasis on critical infrastructure resiliency in the NIPP. Consistent with these changes, DHS has also taken actions to increase its emphasis on resilience in the programs and tools it uses to assess vulnerability and risk that are designed to help asset owners and operators identify resiliency characteristics and gaps. These actions continue to evolve and could be improved if DHS were to strengthen program management by developing measures to assess the extent to which asset owners and operators are taking actions to address resiliency gaps identified during vulnerability assessments; and updating PSA guidelines to articulate PSA roles and responsibilities with regard to resiliency during their interactions with asset owners and operators. By developing performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during the various vulnerability assessments, DHS would, consistent with the NIPP, be better positioned to demonstrate effectiveness in promoting resiliency among the asset owners and operators it works with and would have a basis for analyzing performance gaps. DHS managers would also have a valuable tool to help them assess where problems might be occurring, or alternatively provide insights into the tools used to assess vulnerability and risk and whether they were focusing on the correct elements of resiliency at individual facilities or groups of facilities. Furthermore, by updating PSA guidance to discusses the role PSAs play during interaction with asset owners and operators, including how PSAs can work with them to mitigate vulnerabilities and strengthen their security, DHS would have greater assurance that PSAs are equipped to help asset owners and operators have the tools they need to develop resilience strategies. This would also be consistent with DHS efforts to train PSAs about resiliency and how it affects asset owners and operators.

Related to its efforts to develop or update its programs designed to assess vulnerability at asset owners' and operators' individual facilities and groups of facilities, DHS has considered how it can disseminate information on resiliency practices it gathers or plans to gather with asset owners and operators within and across sectors. However, it faces barriers in doing so because it would have to overcome perceptions that it is

advancing or promoting standards that have to be adopted and concerns about sharing proprietary information. We recognize that DHS would face challenges disseminating information about resiliency practices within and across sectors, especially since resiliency can mean different things to different sectors. Nonetheless, as the primary federal agency responsible for coordinating and enhancing the protection and resiliency of critical infrastructure across the spectrum of CIKR sectors, DHS is uniquely positioned to disseminate this information. By determining the feasibility of overcoming barriers and developing an approach for disseminating resiliency information, DHS could better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments, based on the practices and experiences of their peers within the CIKR community, both within and across sectors.

Recommendations for Executive Action

To better ensure that DHS's efforts to incorporate resiliency into its overall CIKR protection efforts are effective and completed in a timely and consistent fashion, we recommend that the Assistant Secretary for Infrastructure Protection take the following two actions:

- develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during the various vulnerability assessments; and
- update PSA guidance that discusses the role PSAs play during interactions with asset owners and operators with regard to resiliency, which could include how PSAs work with them to emphasize how resiliency strategies could help them mitigate vulnerabilities and strengthen their security posture and provide suggestions for enhancing resiliency at particular facilities.

Furthermore, we recommend that the Secretary of Homeland Security assign responsibility to one or more organizations within DHS to determine the feasibility of overcoming barriers and developing an approach for disseminating information on resiliency practices to CIKR owners and operators within and across sectors.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security for review and comment. In written comments DHS agreed with two of our recommendations and said that it needed additional time to internally consider the third. Regarding our first recommendation that IP develop

performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during vulnerability assessments, DHS said that IP had developed measures on owners' and operators' efforts to implement enhancements to security and resilience, and NPPD officials are reviewing these new performance metrics. With regard to our second recommendation to update guidance that discusses the role PSAs play during interactions with asset owners and operators about resiliency, DHS said that IP is actively updating PSA program guidance to reflect the evolving concept of resilience and will include information on resilience in the next revision to the PSA program management plan. Finally, regarding our third recommendation that DHS assign responsibility to one or more organizations within DHS to determine the feasibility of developing an approach for disseminating information on resiliency practices, DHS said that its components need time to further consider the recommendation and will respond to GAO and Congress at a later date. DHS also provided technical comments which we incorporated as appropriate.

As agreed with your office, 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 send copies of this report to the Secretary of Homeland Security, the Under Secretary for the National Protection Programs Directorate, appropriate congressional committees, and other interested parties. If you have any further questions about this report, please contact me at (202) 512-8777 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Appendix I: Comments from the Department of Homeland Security

U.S. Department of Homeland
Washington, DC 20528

Homeland Security

September 15, 2010

Mr. Stephen L. Caldwell
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Caldwell:

Subject: Draft Report GAO-10-772SU, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving But Program Management Could Be Strengthened* (Job Code 440733)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above. We agree with two of the recommendations directed to the Office of Infrastructure Protection, an office within the National Protection and Programs Directorate (NPPD), but need additional time to internally discuss the third recommendation made to the Department.

Recommendation 1: To better ensure that DHS's efforts to incorporate resiliency into its overall Critical Infrastructure and Key Resources (CIKR) protection efforts are effective and completed in a timely and consistent fashion, GAO recommends that the Assistant Secretary for Infrastructure Protection develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during the various vulnerability assessments.

Response: NPPD/ Office of Infrastructure Protection (IP) concurs with this recommendation. IP, specifically the Protective Security Coordination Division, has already developed performance measures related to assessing the impact of IP assessments on improving the security and resilience of critical infrastructure by measuring the rate at which critical infrastructure owners and operators are implementing improvements to enhance security and resilience. NPPD officials are reviewing these new performance metrics.

Recommendation 2: To better ensure that DHS's efforts to incorporate resiliency into its overall CIKR protection efforts are effective and completed in a timely and consistent fashion, GAO recommends that the Assistant Secretary for Infrastructure Protection update Protective Security Advisor (PSA) guidance that discusses the role PSAs play during interactions with asset owners and operators with regard to resiliency, which could include how PSAs work with them to emphasize how resiliency strategies could help them mitigate vulnerabilities and strengthen their security posture and provide suggestions for enhancing resiliency at particular facilities.

Response: NPPD/IP concurs with this recommendation. The PSA Program is actively updating PSA Program guidance to reflect the evolving concept of critical infrastructure resilience. The PSA Program has introduced resilience into PSA training, facility assessments, and will include resilience in the next revision of the PSA Program Management Plan.

Recommendation 3: GAO recommends that the Secretary of Homeland Security assign responsibility to one or more organizations within the Department of Homeland Security to determine the feasibility of overcoming barriers and developing an approach for disseminating information on resiliency practices to CIKR owners and operators within and across sectors.

Response: The Department's components need to discuss further the recommendation and will provide the Department's decision to GAO and Congress through the 60-day response letter.

Sincerely,

Jerald E. Levine
Director
Departmental GAO-OIG Liaison Office

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-8777 or CaldwellS@gao.gov

Staff Acknowledgments

In addition to the contact named above, John F. Mortin, Assistant Director, and Katrina R. Moss, Analyst-in-Charge, managed this assignment. Katherine M. Davis, Anthony J. DeFrank, Michele C. Fejfar, Tracey L. King, Landis L. Lindsey, Thomas F. Lombardi, Lara R. Miklozek, Steven R. Putansu, Edith N. Sohna, and Alex M. Winograd made significant contributions to the work.

Related GAO Products

Critical Infrastructure Protection

Critical Infrastructure Protection: Updates to the 2009 National Infrastructure Protection Plan and Resiliency in Planning. GAO-10-296. Washington, D.C.: March 5, 2010.

The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. GAO-09-654R. Washington, D.C.: June 26, 2009.

Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination. GAO-08-36. Washington, D.C.: October 31, 2007.

Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving. GAO-07-1075T. Washington, D.C.: July 12, 2007.

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

Critical Infrastructure: Challenges Remain in Protecting Key Sectors. GAO-07-626T. Washington, D.C.: March 20, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. Washington, D.C.: October 16, 2006.

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

Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed. GAO-02-781. Washington, D.C.: August 30, 2002.

Cyber Security

Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. GAO-09-969. Washington, D.C.: September 24, 2009.

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks. GAO-08-607. Washington, D.C.: June 26, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. GAO-08-64T. Washington, D.C.: October 31, 2007.

Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies. GAO-08-113. October 31, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

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

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

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

Critical Infrastructure Protection: 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.

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

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.

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

High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. GAO-03-121. Washington, D.C.: January 1, 2003.

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

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T. Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T. Washington, D.C.: May 22, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323. Washington, D.C.: April 25, 2001.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. GAO/T-AIMD-00-229. Washington, D.C.: June 22, 2000.

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities. GAO/T-AIMD-00-181. Washington, D.C.: May 18, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. GAO/AIMD-00-90R. Washington, D.C.: February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. GAO/T-AIMD-00-72. Washington, D.C.: February 1, 2000.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. GAO/T-AIMD-00-7. Washington, D.C.: October 6, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD-00-1. Washington, D.C.: October 1, 1999.

Defense Critical Infrastructure Protection

Defense Critical Infrastructure: Actions Needed to Improve Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets. GAO-10-147. October 23, 2009.

Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List. GAO-09-740R. Washington, D.C.: July 17, 2009.

Defense Critical Infrastructure: Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure. GAO-09-42. Washington, D.C.: October 30, 2008.

Defense Critical Infrastructure: Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets. GAO-08-851. Washington, D.C.: August 15, 2008.

Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets. GAO-08-373R. Washington, D.C.: April 2, 2008.

Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base. GAO-07-1077. Washington, D.C.: August 31, 2007.

Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure. GAO-07-461. Washington, D.C.: May 24, 2007.

Electrical Power

Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance. GAO-08-987. Washington, D.C.: September 22, 2008.

Department of Energy, Federal Energy Regulatory Commission: Mandatory Reliability Standards for Critical Infrastructure Protection. GAO-08-493R. Washington, D.C.: February 21, 2008.

Electricity Restructuring: Key Challenges Remain. GAO-06-237. Washington, D.C.: November 15, 2005.

Meeting Energy Demand in the 21st Century: Many Challenges and Key Questions. GAO-05-414T. Washington, D.C.: March 16, 2005.

Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection. GAO-03-586. Washington, D.C.: June 30, 2003.

Restructured Electricity Markets: Three States' Experiences in Adding Generating Capacity. GAO-02-427. Washington, D.C.: May 24, 2002.

Energy Markets: Results of FERC Outage Study and Other Market Power Studies. GAO-01-1019T. Washington, D.C.: August 2, 2001.

Other

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO-03-519T. Washington, D.C.: March 3, 2003.

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

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

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548