

March 2010

# CRITICAL INFRASTRUCTURE PROTECTION

Update to National  
Infrastructure  
Protection Plan  
Includes Increased  
Emphasis on Risk  
Management and  
Resilience



GAO

Accountability \* Integrity \* Reliability



Highlights of [GAO-10-296](#), a report to congressional requesters

## Why GAO Did This Study

According to the Department of Homeland Security (DHS), there are thousands of facilities in the United States that if destroyed by a disaster could cause casualties, economic losses, or disruptions to national security. The Homeland Security Act of 2002 gave DHS responsibility for leading and coordinating the nation's effort to protect critical infrastructure and key resources (CIKR). Homeland Security Presidential Directive 7 (HSPD-7) defined responsibilities for DHS and certain federal agencies—known as sector-specific agencies (SSAs)—that represent 18 industry sectors, such as energy. In accordance with the Homeland Security Act and HSPD-7, DHS issued the National Infrastructure Protection Plan (NIPP) in June 2006 to provide the approach for integrating the nation's CIKR. GAO was asked to study DHS's January 2009 revisions to the NIPP in light of a debate over whether DHS has emphasized protection—to deter threats, mitigate vulnerabilities, or minimize the consequences of disasters—rather than resiliency—to resist, absorb, or successfully adapt, respond to, or recover from disasters. This report discusses (1) how the 2009 NIPP changed compared to the 2006 NIPP and (2) how DHS and SSAs addressed resiliency as part of their planning efforts. GAO compared the 2006 and 2009 NIPPs, analyzed documents, including NIPP Implementation Guides and sector-specific plans, and interviewed DHS and SSA officials from all 18 sectors about their process to identify potential revisions to the NIPP and address resiliency.

View [GAO-10-296](#) or [key components](#). For more information, contact Stephen L. Caldwell at (202) 512-8777 or [caldwells@gao.gov](mailto:caldwells@gao.gov).

## CRITICAL INFRASTRUCTURE PROTECTION

### Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience

#### What GAO Found

Compared to the 2006 NIPP, DHS's 2009 update to the NIPP incorporated various changes, including a greater emphasis on regional CIKR protection planning and updates to DHS's overall risk management framework, such as instructions for sectors to develop metrics to gauge how well programs reduced the risk to their sector. For example, in the 2006 NIPP, DHS encouraged stakeholders to address CIKR across sectors within and across geographic regions; by contrast, the 2009 NIPP called for regional coordination through the formation of a consortium of representatives from multiple regional organizations. DHS also enhanced its discussion of risk management methodologies in the 2009 NIPP. The 2006 NIPP listed the minimum requirements for conducting risk analyses, while the 2009 NIPP includes the use of a common risk assessment approach, including the core criteria for these analyses to allow the comparison of risk across sectors. DHS officials said that the changes highlighted in the 2009 NIPP were the result of knowledge gained and issues raised during discussions with partners and outside organizations like GAO. DHS has also issued guidance for SSAs to consider revisions to the NIPP when updating their sector-specific plans (SSPs). Fourteen of 18 SSA representatives that responded to our query said they used a process similar to DHS's to incorporate NIPP changes into their SSPs. They reported that they intend to discuss the expectations for the SSP with DHS, draft the SSP based on their knowledge of their sectors, and obtain input and feedback from stakeholders.

DHS increased its emphasis on resiliency in the 2009 NIPP by discussing it with the same level of importance as protection. While the 2009 NIPP uses much of the same language as the 2006 NIPP to describe resiliency, the 2006 NIPP primarily treated resiliency as a subset of protection while the 2009 NIPP generally referred to resiliency alongside protection. For example, while the Managing Risk chapter of the 2006 NIPP has a section entitled "Characteristics of Effective Protection Programs," the same chapter in the 2009 NIPP has a section entitled, "Characteristics of Effective Protection Programs and Resiliency Strategies." DHS officials stated that these changes are not a major shift in policy; rather they are intended to raise awareness about resiliency as it applies within individual sectors. Furthermore, they stated that there is a greater emphasis on resiliency in the 2009 NIPP to encourage more sector and cross-sector activities to address a broader spectrum of risks, such as cyber security. DHS officials also used guidance to encourage SSAs to devote more attention to resiliency. For example, in the 2009 guidance, SSAs are advised that in sectors where infrastructure resiliency is as or more important than physical security, they should focus on describing the resiliency measures and strategies being used by the sector. The 2010 updates to the SSPs are due to be released by DHS in mid-2010 and all sector representatives who responded to our questions said they will address the issue as is appropriate for their sectors. In commenting on a draft of this report, DHS reiterated its process for updating the NIPP and its views on resiliency.

---

# Contents

---

<b>Letter</b>		1
	Background	6
	DHS Has Incorporated Changes into the 2009 NIPP that Reflect Stakeholder Input and Sectors' Experience Protecting Critical Infrastructure and an Increased Emphasis on Risk Management	10
	DHS Increased Its Emphasis on Resiliency in the 2009 NIPP and Directed SSAs to Address Resiliency in Their Sector Plans	22
	Agency Comments	27
<b>Appendix I</b>	<b>The Concept of Resiliency</b>	29
<b>Appendix II</b>	<b>Discussions of Resiliency in 2007 Sector-specific Plans</b>	32
<b>Appendix III</b>	<b>Comments from the Department of Homeland Security</b>	36
<b>Appendix IV</b>	<b>GAO Contacts and Acknowledgments</b>	36
<b>GAO Products</b>	<b>Related to Critical Infrastructure Protection</b>	38
<b>Tables</b>		
	Table 1: SSAs and CIKR Sectors	8
	Table 2: Description of Changes Made from the 2006 NIPP to the 2009 NIPP	10
	Table 3: Sector Plan References to Resiliency	33
<b>Figures</b>		
	Figure 1: DHS Process to Update the NIPP	16
	Figure 2: Process for updating SSPs	19

---

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

March 5, 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

According to the Department of Homeland Security (DHS), there are thousands of facilities in the United States that if degraded or destroyed by a manmade or natural disaster could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity. There are also networks and systems—including cyber networks that support physical infrastructure—that are vulnerable and valuable. Damages to these facilities, networks, and systems and the economic impact of their destruction could easily run into the billions of dollars.

The Homeland Security Act of 2002 created DHS and gave the department wide-ranging responsibilities for, among other things, leading and coordinating the overall national critical infrastructure protection effort.<sup>1</sup> For example, the act required DHS to (1) develop a comprehensive national plan for securing the nation's critical infrastructures and key resources (CIKR) and (2) recommend measures to protect CIKR in coordination with other agencies of the federal government and in cooperation with state and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 (HSPD-7) further defined critical infrastructure protection responsibilities for DHS and those federal agencies—known as sector-specific agencies (SSA)—responsible for particular industry sectors, such

---

<sup>1</sup>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.

---

as transportation, energy, and communications.<sup>2</sup> For example, the Department of the Treasury as the SSA is responsible for the banking and finance sector while the Department of Energy as the SSA is responsible for the energy sector. HSPD-7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across 17 sectors. The directive also gave DHS the authority to establish additional sectors and in 2008, DHS created an 18<sup>th</sup> sector for critical manufacturing. We placed the protection of the federal government's information systems and the nation's critical infrastructures on our high-risk list in 1997.<sup>3</sup> We consider this area high risk because federal agencies and our nation's critical infrastructures—such as power distribution, water treatment and supply, telecommunications, national defense, and emergency services—rely extensively on computerized information systems and electronic data to carry out their operations. The security of these systems and data is essential to preventing disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Protecting federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection, or cyber CIP—is a continuing concern.

In accordance with the Homeland Security Act and in response to HSPD-7, DHS issued, in June 2006, the first National Infrastructure Protection Plan (NIPP), which provides the overarching approach for integrating the nation's CIKR protection initiatives in a single effort.<sup>4</sup> DHS issued a revised NIPP in January 2009.<sup>5</sup> The NIPP sets forth a risk management framework

---

<sup>2</sup>The 18 sectors are Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Public Health and Healthcare; Transportation Systems and Water.

<sup>3</sup>In 1990, we began a program to report on government operations that it 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 *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009). Cyber security is the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability.

<sup>4</sup>DHS, National Infrastructure Protection Plan (Washington, D.C.: June 2006).

<sup>5</sup>DHS, National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency (Washington, D.C.: January 2009).

---

and details the roles and responsibilities of DHS, SSAs, and other federal, state, regional, local, tribal, territorial, and private sector partners, including how they should use risk management principles to prioritize protection activities within and across sectors.<sup>6</sup> 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 private sector and DHS.<sup>7</sup> 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 sector-specific agency; a government coordinating council to represent each sector's interests among government agencies; and a sector coordinating council<sup>8</sup> that includes private sector representatives of the sector.<sup>9</sup> Each sector is responsible for developing sector-specific plans (SSPs) and sector annual reports (SARs). In 2007, each SSA then operating published an SSP that mirrored and applied the NIPP framework. SSPs are to be updated, like the NIPP, every 3 years and the second iteration of

---

<sup>6</sup>According to DHS, 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; and measuring performance, and taking corrective action.

<sup>7</sup>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 DHS's effort to comply with a congressional mandate that directed it to complete an analysis of 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 entities to provide sensitive information to the department conflicts with the voluntary information-sharing approach DHS was to pursue under the Homeland Security Act.

<sup>8</sup>The Government Facilities and National Monuments and Icons Sectors do not have Sector Coordinating Councils due to the fact that they are uniquely governmental.

<sup>9</sup>The Government Coordinating Council comprises representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the risk and scope of each individual sector. The sector coordinating council is the private sector counterpart to the government coordinating councils. The private sector councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. Sector coordinating councils 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.

---

SSPs is due in 2010.<sup>10</sup> In addition, beginning in 2006 each sector then operating was to produce a SAR that is expected to focus on sector goals, priorities, and SSP implementation.

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. CIKR partners in the public and the private sector 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 framing the debate over this issue, the National Infrastructure Advisory Council stated that:

“The challenge facing government is to maintain its role in protecting critical infrastructures, while determining how best to encourage market forces to improve the resilience of companies, provide appropriate incentives and tools to help entire sectors become resilient, and step in when market forces alone cannot produce the level of infrastructure security needed to protect citizens, communities, and essential economic systems.”<sup>11</sup>

Given the debate over DHS's emphasis on protection rather than resilience, you asked us to study DHS's revisions to the NIPP and efforts by DHS to address resiliency as part of its national planning efforts. Specifically, this report addresses the following questions

1. How has the 2009 NIPP changed compared to the 2006 NIPP and what process was used to identify and incorporate these changes? and
2. How have DHS and SSAs addressed the concept of critical infrastructure resiliency as part of their national CIKR and sector-specific planning efforts?

---

<sup>10</sup>The SSPs provide the means by which the NIPP is implemented across all 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. The Critical Manufacturing sector will produce its first SSP in 2010. The SARs 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.

<sup>11</sup>National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations* (Washington, D.C.: Sept. 8, 2009).

---

To describe the changes DHS has made to the NIPP since it was first published in 2006 and the process used to identify and incorporate these changes, we compared the 2006 and 2009 versions of the NIPP and reviewed the changes that have occurred. We also interviewed DHS NIPP Program Management Office (PMO) officials responsible for developing and coordinating the NIPP revisions to discuss the process they used to identify potential revisions and why changes were made. We analyzed DHS's 2006 and 2009 SSP guidance that supports the NIPP to determine what changes were made in the 2009 guidance which is designed to help ensure that SSAs develop SSPs consistent with the 2009 NIPP. Furthermore, we interviewed NIPP PMO officials about their efforts to work with SSAs in developing plans and reports based on the guidance provided and asked SSAs about the process they used to address changes to the NIPP in their SSPs. We also interviewed SSA representatives for all 18 critical infrastructure sectors and asked them how they planned to address the changes to the NIPP in their 2010 SSPs.

To determine how DHS and the SSAs have addressed the concept of critical infrastructure resiliency as part of their national CIKR protection planning efforts, we collected and analyzed documentary and testimonial evidence from DHS and SSAs. Specifically, we reviewed the 2006 and 2009 NIPP and the NIPP Implementation Guides to compare how often and in what context the concept of resiliency was used between those dates of publication. We limited our analysis to how often and where resiliency-related terms—resilience, resiliency, resilient, and continuity (business or operational continuity)—were used in the plans and corresponding guidance. In commenting on our approach, DHS said this is a reasonable set of terms for our analysis.<sup>12</sup> We also reviewed the sector-specific planning documents (e.g., SSPs) of the sectors that were issued based on the 2006 NIPP Implementation Guide and assessed how the concept of resiliency was addressed by the individual sectors. Finally, we interviewed SSA officials for all 18 sectors to determine how they plan to address the concept of resiliency in their 2010 SSPs.<sup>13</sup>

---

<sup>12</sup>NIPP PMO officials said the NIPP treats protection and resilience as related concepts—not mutually exclusive ones, so strictly looking at word counts will not identify all the changes. However, as noted above and as agreed with DHS, our analysis took into account where and in what context these terms were used.

<sup>13</sup>Not all sector representatives answered each question regarding sector plans to address changes in the NIPP and the direction to address resiliency in their 2010 sector-specific plans. Thus, when discussing sector representative responses in this report, we identify the number of sectors that responded.

---

We conducted this performance audit from August 2009 through February 2010 in accordance with generally accepted auditing standards. These 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 NIPP provides the framework for developing, implementing, and maintaining a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners to manage the risks to CIKR. In addition to the Homeland Security Act, various statutes provide legal authority for both cross-sector and sector-specific protection and resiliency programs. For example, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 was intended to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies and the Pandemic and All-Hazards Preparedness Act addresses public health security and all-hazards preparedness and response.<sup>14</sup> Also, the Cyber Security Research and Development Act of 2002 authorized funding for the National Institute of Standards and Technology (NIST) and the National Science Foundation to facilitate increased research and development for computer and network security and to support research fellowships and training.<sup>15</sup> CIKR protection issues are also covered under various presidential directives, including HSPD-5 and HSPD-8. 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

---

<sup>14</sup>Pub. L. No. 107-188, 116 Stat. 594 (2002); Pub. L. No. 109-417, 120 Stat. 2831 (2006).

<sup>15</sup>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); 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.

---

emergencies.<sup>16</sup> 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 other security partners—including other federal agencies, state, territorial, local, 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. The NIPP is prepared by the NIPP Program Management Office (PMO) within the Infrastructure Protection office of the National Preparedness and Protection Directorate of DHS. The NIPP PMO has the responsibility for coordinating and ensuring development, implementation, and maintenance of the NIPP and the associated sector-specific plans.

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 CIKR sectors. The remaining sectors are coordinated by eight other federal agencies. The NIPP depends on supporting SSPs for full implementation of this framework within and across CIKR sectors. SSPs are developed by the SSAs designated in HSPD-7 in close collaboration with sector partners, including sector and government coordinating councils. These SSPs contain the plan to identify and address the risks to CIKR specific to each sector and are reviewed by DHS for adherence to DHS guidance which follows the format of the NIPP. Table 1 lists the SSAs and their sectors.

---

<sup>16</sup>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**

<b>Sector-specific agency</b>	<b>Critical infrastructure and key resource sector</b>
Departments of Agriculture <sup>a</sup> and Food and Drug Administration <sup>b</sup>	Agriculture and Food
Department of Defense <sup>c</sup>	Defense Industrial Base
Department of Energy	Energy <sup>d</sup>
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 <sup>e</sup>
Department of Homeland Security	
• Office of Infrastructure Protection	Commercial Facilities Critical Manufacturing Emergency Services Nuclear Reactors, Materials, and Waste Dams and 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 <sup>f</sup>	Transportation Systems <sup>g</sup>
• Federal Protective Service <sup>h</sup>	Government Facilities <sup>i</sup>

Source: 2009 National Infrastructure Protection Plan.

<sup>a</sup>The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

<sup>b</sup>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.

<sup>c</sup>Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), 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.

<sup>d</sup>The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

<sup>e</sup>The Water Sector includes drinking water and wastewater systems.

<sup>f</sup>The U.S. Coast Guard is the SSA for the maritime transportation mode within the Transportation System Sector.

<sup>g</sup>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.

<sup>h</sup>As of October 2009, the Federal Protective Service transitioned out of Immigration and Customs Enforcement (ICE) to the National Protection and Programs Directorate.

<sup>i</sup>The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

---

The concept of resilience 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 February 2006, the Task Force of the Homeland Security Advisory Council defined resiliency as "the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must."<sup>17</sup> Later in 2006, the Department of Homeland Security's National Infrastructure Protection Plan defined resilience as "the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident."

In May 2007 the President issued Homeland Security Presidential Directive 20—National Continuity Policy. This directive establishes a comprehensive national policy on the continuity of federal government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of federal continuity policies. It also directs executive departments and agencies to integrate continuity requirements into operations, and provides guidance for state, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency. As part of Homeland Security Presidential Directive 20, the Secretary of Homeland Security is directed to, among other things, coordinate the implementation, execution, and assessment of continuity operations and activities; develop, lead, and conduct a federal continuity training and exercise program, which shall be incorporated into the National Exercise Program; and develop and promulgate continuity planning guidance to state, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators.<sup>18</sup> For additional discussion of the concept of resiliency, see appendix 1.

---

<sup>17</sup>The Homeland Security Advisory Council provides advice, recommendations, and expertise to the government regarding protection policy and activities.

<sup>18</sup>DHS coordinates the National Exercise Program which is designed to ensure the nation's readiness to respond to terrorist and natural disasters and to practice and evaluate protection plans and programs put in place by the NIPP.

## DHS Has Incorporated Changes into the 2009 NIPP that Reflect Stakeholder Input and Sectors' Experience Protecting Critical Infrastructure and an Increased Emphasis on Risk Management

DHS incorporated changes in the 2009 NIPP—including a greater emphasis on CIKR regional planning and updates to DHS's overall risk management framework—that NIPP PMO officials said are based on stakeholder input and sectors' experiences performing critical infrastructure protection. Based on DHS guidance, SSAs are expected to address many of the changes to the NIPP in their SSPs, based on consultation with sector partners. Table 2 provides an overview of key changes to the NIPP.

**Table 2: Description of Changes Made from the 2006 NIPP to the 2009 NIPP**

Type of change	2006 NIPP	Change to the 2009 NIPP
Scope of critical infrastructure	The 2006 NIPP defined processes and mechanisms used to prioritize protection within 17 CIKR sectors.	The 2009 NIPP continued to address CIKR prioritization and introduced the Critical Manufacturing sector.
Coordination	The 2006 NIPP created the sector partnership model as the primary organizational structure for coordinating CIKR efforts and activities. The model encouraged Sector and Government Coordinating Councils to work in tandem to create a coordinated national framework for CIKR protection within and across sectors.	The 2009 NIPP expanded the sector partnership model to include Regional Consortium Coordinating Councils. These councils are to coordinate physical security, cybersecurity, emergency preparedness, and overall public-private continuity and resiliency in one or more states, urban areas, or municipalities.
	The 2006 NIPP created a Web-based, information-sharing network so that security partners can obtain, analyze, and share information.	The 2009 NIPP expanded information sharing at the local level via State and Local Fusion Centers to include the critical infrastructure protection mission. These fusion centers are to develop capabilities to support a comprehensive understanding of threats, local CIKR vulnerabilities, and potential consequences of attacks on business operations within the private sector.

Type of change	2006 NIPP	Change to the 2009 NIPP
Planning	The 2006 NIPP created a risk management framework – establishing the process for combining consequence, vulnerability, and threat information to produce a comprehensive assessment of national or sector-specific risk that drives CIKR protection activities.	The 2009 NIPP highlighted updates to risk methodologies and information-sharing mechanisms. The plan also highlighted new outcome-focused performance measurement and reporting processes to measure program performance.
	The 2006 NIPP created a framework to enable education, training, and exercise programs that allow people and organizations to develop and maintain key CIKR protection expertise.	The 2009 NIPP highlighted expanded CIKR protection-related education, training, outreach, and exercise programs. For example, one expanded program provides the framework for the identification, development, and delivery of critical infrastructure courses for the transportation industry.
	The 2006 NIPP primarily focused on CIKR protection strategies.	The 2009 NIPP continued to focus on CIKR protection but placed more emphasis on the concept of resilience. The term resilience also appeared prominently throughout the NIPP.
Supporting laws, strategies, and directives	The 2006 NIPP provided information on a variety of statutes, strategies, and directives applicable to CIKR protection.	The 2009 NIPP provided updated information on legislation, strategies, and directives applicable to CIKR protection.

Source: GAO analysis of the 2006 and 2009 National Infrastructure Protection Plans.

## DHS Changes to the 2009 NIPP Include Increased Emphasis on Regional Planning and Risk Management

DHS changes to the 2009 NIPP include increased emphasis on regional planning and risk management and, according to PMO officials, these changes are based on stakeholder input and sectors’ experiences performing critical infrastructure protection. The changes we identified in the 2009 NIPP were generally foreshadowed in the 2007/2008 NIPP Update provided to SSAs in 2008.<sup>19</sup> While most of the changes in the 2009 NIPP were minor and related to changes in programs or activities that have occurred since the publication of the 2006 NIPP, several could have an impact on the sector planning process and the development of SSPs. These included changes that placed a greater emphasis on regional planning, coordination and information-sharing across sectors; changes in how critical infrastructures are identified and prioritized; developments in risk management to include how threats, vulnerabilities, and

<sup>19</sup>The 2007/2008 NIPP Update was released in August 2008 and captured changes to infrastructure protection that occurred since the release of the 2006 NIPP.

---

consequences are assessed; and a greater emphasis on cyber security and international interdependencies.

In contrast to the 2006 NIPP, DHS increased its emphasis on regional planning, coordination and information-sharing in the 2009 NIPP. DHS discussed the need for regional coordination in the 2006 NIPP and encouraged stakeholders to address CIKR protection across sectors within and across geographic regions. In the 2006 NIPP, regional bodies were to be formed on an “as needed” basis. By contrast, the 2009 NIPP called for regional coordination through the formation of a consortium of representatives from multiple regional organizations. The 2009 NIPP states that this was done to help enhance the engagement of regionally based partners and to leverage the CIKR protection activities and resiliency strategies that they lead.

In comparison to the 2006 NIPP, DHS included a discussion of changes in how critical infrastructures are identified and prioritized in the 2009 NIPP. Both the 2006 NIPP and the 2009 NIPP stated that CIKR inventory lists were developed from multiple sources, including sector inventories maintained by SSAs and government coordinating councils, voluntary submissions from CIKR partners in the public or private sector, and the results of studies conducted by various trade associations, advocacy groups, and regulatory agencies. While the 2006 NIPP briefly discusses its efforts to determine which assets are nationally critical, the 2009 NIPP includes a more detailed discussion of the national CIKR prioritization program that places CIKR into categories according to their importance, nationally or regionally. Specifically, DHS prioritized assets using a tiered approach. Tier 1 or Tier 2 assets are those that if destroyed or disrupted could cause 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 Tier 2. Only a small subset of assets meet the Tier 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.<sup>20</sup>

DHS also provided a detailed discussion of risk management methodologies in the 2009 NIPP, as compared to the 2006 NIPP. Whereas the 2006 NIPP listed the baseline criteria—minimum requirements—for conducting risk analyses to ensure they are credible and comparable, the 2009 NIPP includes the use of a common risk assessment approach, including the core criteria—updated requirements—for threat, vulnerability, and consequence analyses designed to allow the comparison of risk across sectors. For example, regarding consequence assessments, the 2006 NIPP discusses the use of consequence screening to help CIKR owners and operators determine whether it is necessary to provide additional information to DHS or the SSA. Consequence screening is an approach that allows CIKR owners and operators to identify their projected level of consequence based on the nature of their business, proximity to significant populations or other CIKR, relative importance to the national economy or military capability, and other similar factors. In contrast the 2009 NIPP includes a discussion of consequence uncertainty where a range of outcomes is possible. The 2009 NIPP states that where the range of outcomes is large, greater detail may be required to calculate consequence and inform decisionmaking. As part of this risk management discussion, DHS has also made changes regarding how sectors are to measure the performance of their CIKR programs. While both the 2006 and 2009 NIPP discuss descriptive and process or output data, the 2009 NIPP included additional discussion regarding the development of metrics that assess how well programs reduced the risk to the sector.<sup>21</sup> The 2009 NIPP also discusses changes made to the approach for conducting these assessments. For example, whereas the 2006 NIPP

---

<sup>20</sup>The process of identifying these nationally significant assets and systems is conducted on an annual basis and relies heavily on the insights and knowledge of a wide array of public and private sector security partners. CIKR categorized as Tier 1 or Tier 2 as a result of this annual process provide a common basis on which DHS and its security partners can implement important CIKR protection programs and initiatives, such as various grant programs, buffer zone protection efforts, facility assessments and training, and other activities. DHS has other tiered categories of infrastructure whose destruction or disruption would not have a significant national or regional impact, though local impacts could be substantial.

<sup>21</sup>Examples of descriptive data include the number of facilities in a jurisdiction and the number of suppliers in an infrastructure service provider's supply chain. Examples of process or output data include the number of protective programs implemented in a fiscal year and the percentage of sector organizations exchanging CIKR information.

---

focused on facility vulnerability assessments, the 2009 NIPP discusses broader assessment efforts, including DHS's efforts to conduct a systemwide vulnerability assessment. To illustrate a systemwide vulnerability assessment, DHS used the example of the California Water System Comprehensive Review, a DHS-led assessment effort to identify critical water system assets, analyze and track the gaps in protection, and identify potential enhancements.

In addition, DHS included a greater emphasis on cyber security in the 2009 NIPP than it did in the 2006 NIPP. The 2006 NIPP identified cross-sector cyber security as an area worthy of special consideration by the sectors. In comparison, the 2009 NIPP lists the progress made and new initiatives related to cyber security, including the development of cross-sector cyber methodologies to identify systems or networks of national significance; the addition of a cross-sector cyber security working group and a public-private cross-sector program specifically for cyber security. The 2009 NIPP also lists new responsibilities for CIKR partners to conduct cyber security exercises to test the security of these systems as well as the development of cyber security-specific vulnerability assessments by DHS.

Furthermore, in contrast to the 2006 NIPP, DHS also expanded its emphasis on international coordination and identified it as an area warranting special consideration in the 2009 NIPP. Whereas the 2006 NIPP highlighted the importance of international coordination, the 2009 NIPP instructs the SSAs to identify foreign critical infrastructure—whether American owned or foreign owned—of national importance, and lists the procedures for doing so. The 2009 NIPP discusses the importance of identifying and prioritizing infrastructure located outside the United States that if disrupted or destroyed would have a negative impact on the United States, lists additional SSA responsibilities for international coordination, and lists various international organizations that are assisting in the implementation of international CIKR agreements. The 2009 NIPP also highlights DHS's role in a 15-nation effort specific to cyber security.

NIPP PMO officials said that the changes highlighted in the 2009 NIPP were the result of knowledge gained and issues raised during regularly scheduled—bimonthly or quarterly—or specially called meetings with security partners such as the Federal Senior Leadership Council, the CIKR Cross-Sector Council, and other contacts with security partners such as SSAs, sector coordinating councils, and government coordinating

---

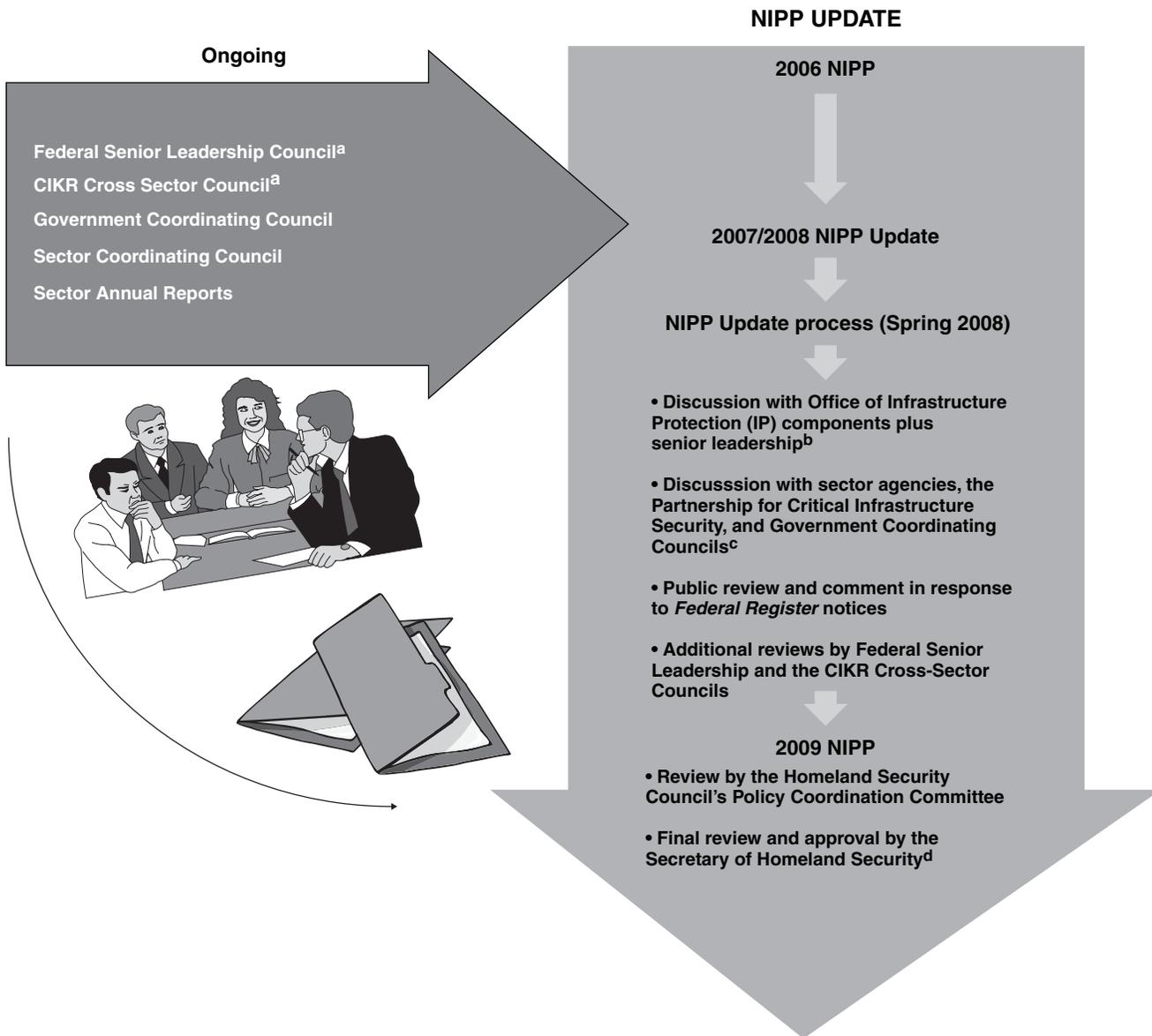
councils.<sup>22</sup> DHS said concerns on CIKR issues were also elevated to DHS based on their inclusion in Sector CIKR Protection Annual Reports, as well as from outside organizations like GAO which NIPP PMO officials credited for the increased attention to cyber security.<sup>23</sup> NIPP PMO officials said DHS began an effort to revise the NIPP in the Spring of 2008 and as part of this process, DHS held discussions with infrastructure protection components and senior leadership. Figure 1 shows the process DHS used to update the NIPP for publication in 2009.

---

<sup>22</sup>The NIPP Federal Senior Leadership Council is composed of representatives of each of the sector-specific agencies to enhance communication and coordination between and among these agencies. The CIKR Cross-Sector Council is made up of representatives from each of the SSAs to address issues that affect multiple sectors.

<sup>23</sup>See GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, [GAO-08-64T](#) (Washington, D.C.: Oct. 31, 2007). GAO, *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, [GAO-09-969](#) (Washington, D.C.: September 2009).

**Figure 1: DHS Process to Update the NIPP**



Source: GAO analysis of DHS information, Art Explosion clipart (images).

<sup>a</sup>The Federal Senior Leadership Council is composed of representatives of each of the sector-specific agencies to enhance communication and coordination between and among these agencies. The CIKR Cross-Sector Council is made up of representatives from each of the SSAs to address issues that affect multiple sectors.

<sup>b</sup>The Office of Infrastructure Protection (IP) leads the coordinated national program to reduce risks to the nation's CIKR posed by acts of terrorism, and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

---

<sup>c</sup>The Partnership for Critical Infrastructure Security coordinates cross-sector initiatives to support CIKR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CIKR protection.

<sup>d</sup>The Homeland Security Council Policy Coordinating Committee coordinates the development and implementation of homeland security policies by multiple departments and agencies throughout the federal government, and coordinates those policies with state and local government.

NIPP PMO officials said that because they view NIPP updates as an ongoing process, they will continue to reassess the NIPP and make changes based on knowledge gained from the various partners and stakeholders, as needed. For example, between the release of the 2006 and 2009 NIPP DHS issued the 2007/2008 NIPP Update. The 2007/2008 NIPP Update contained references to changes that ultimately appeared in the 2009 NIPP, including the introduction of the system used to gather and distribute information on critical infrastructure assets, the process used to develop metrics to measure performance and progress in critical infrastructure protection, and the emphasis on regional coordination in the partnership model. The 2007/2008 NIPP Update also included discussion of a training needs assessment DHS conducted which was followed by the creation of the CIKR competency areas that define CIKR training requirements in the 2009 NIPP.

---

## DHS Guidance Calls for SSAs to Develop Plans and Reports That Consider Specific Issues in the 2009 NIPP

Following the publication of the 2009 NIPP, DHS issued guidance to the SSAs designed to make them aware of the changes to the NIPP and to discuss the issues DHS believed SSAs should consider for increased attention when developing their SSPs and SARs.<sup>24</sup> The guidance provided section-by-section instructions that discussed how SSAs were to update their plans and annual reports to be consistent with the NIPP. For example, the 2010 SSP guidance stated that the NIPP had increased emphasis on DHS's all-hazards approach to CIKR protection planning and suggested that SSPs should place increased emphasis on their approach to addressing all-hazards events when updating their plans. The guidance also noted that SSAs should give additional attention to topics such as cyber security and international interdependencies. Regarding cyber security, the guidance calls for SSAs to include goals or long-term objectives for cyber security in their sector and explain their approach for

---

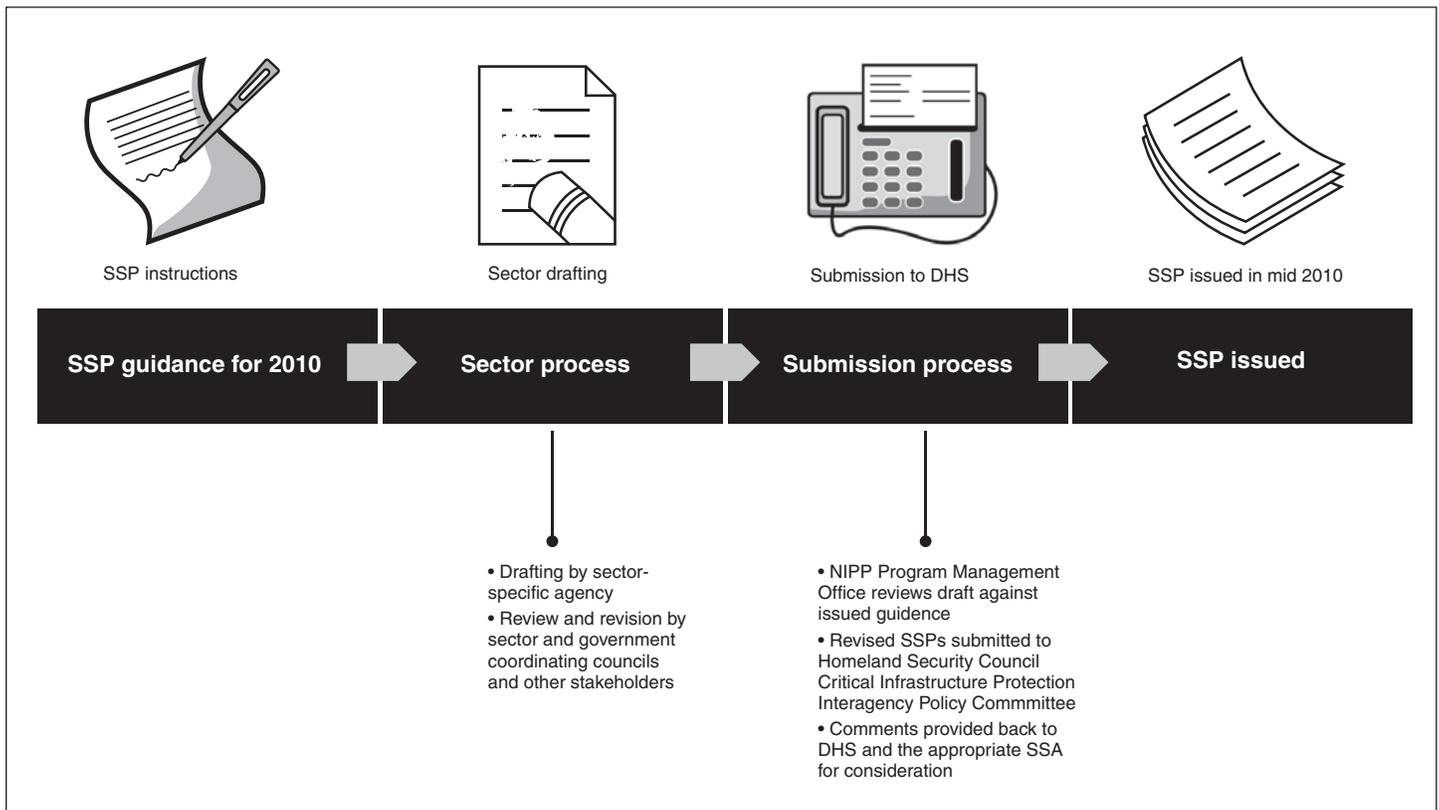
<sup>24</sup>DHS's guidance are the *2009 Sector Critical Infrastructure and Key Resources Protection: Annual Report Guidance* (February 2009); the *Triennial Rewrite and Reissue of the 2010 Sector-Specific Plans: Guidance for Sector-Specific Agencies and Other Sector Partners* (March 2009); and the *2009 Sector Critical Infrastructure and Key Resources Protection: NIPP Metric Guidance* (February 2009).

---

identifying their sector's cyber assets, systems, networks, and functions; incorporating cyber elements into sector risk assessments; and prioritizing cyber elements—such as communication and computer networks—of the sector, among other things.

Fourteen of 18 SSA representatives generally described the process they plan to use to incorporate these changes, which for the most part mirrored DHS's process for revising the NIPP. According to the SSA representatives, after reviewing the guidance provided by DHS, the SSAs plan to employ internal teams or offices to draft the SSP following DHS's format; the SSAs intend to provide the draft to key stakeholders, such as the sector's government coordinating council and sector coordinating council, who are to provide feedback and comments on the draft via e-mail, individual and conference calls, and in-person meetings; and the SSAs plan to make revisions and distribute the draft to stakeholders for final review before submission to DHS. See figure 2 for a description of this process.

**Figure 2: Process for updating SSPs**



Source: GAO analysis of DHS information.

Four of 18 SSA representatives who responded to our inquiries specifically described how changes to the 2009 NIPP either had already been addressed in their 2007 SSPs or would be addressed in the 2010 SSPs. Regarding changes to risk assessment methodologies, for example, the SSA representative for the Water sector stated that three risk assessment tools are available to the Water sector. Furthermore, according to this representative, DHS and its partners are working collaboratively to ensure these existing assessment methodologies are upgraded and revised by using consistent vulnerability, consequence, and threat information, resulting in analysis of risk that is comparable within the sector. The SSA representative said revisions to these tools are to also address the features and elements of risk assessments as identified in the NIPP. The Energy SSA representative also described sector efforts in these areas, including in regional coordination, training and education, international coordination, and cyber security.

---

Those sector officials who did not offer specifics on how they expect to address changes suggested by DHS either provided a general statement of their efforts or said this was because the SSPs were being drafted during our review. Four of the 18 SSA representatives said they have contacted or plan to contact DHS about sector concerns regarding the NIPP format or questions about the instructions provided. For example, the SSA representative for the Healthcare and Public Health sector told us that his agency planned to contact DHS to discuss a change that is designed to make the SSP risk assessment methodology consistent with the NIPP, but could be impractical for the SSA to implement. The Healthcare sector representative said a single risk assessment methodology would not be feasible for the Healthcare and Public Health sector because it is composed of different kinds of partners, such as emergency medical personnel, doctors, and hospitals and is made up of systems—transportation, communication, personnel—as opposed to other sectors which he said may be made up predominantly of facilities. The SSA representative said this makes the use of a single risk assessment methodology difficult for the Healthcare sector. All 14 SSA representatives who responded with a description of the SSP update process said they are taking extra actions to ensure other stakeholder views are considered. For example, the Commercial Facilities SSA said it plans to post a copy of its draft on the Homeland Security Information Network to ensure that sector interests are broadly represented in the review of the document.<sup>25</sup> Another example came from the Dams SSA official who said that his office provided its draft to a dozen organizations and trade associations outside its sector coordinating council and government coordinating council including the American Society of Civil Engineers, the National Dam

---

<sup>25</sup>The Homeland Security Information Network (HSIN) is a national, Web-based communications platform that allows: DHS; SSAs; state, local, tribal, and territorial governmental entities; and other partners to obtain, analyze, and share information. The Critical Sectors element of HSIN is an information-sharing portal designed to encourage communication and collaboration among all CIKR sectors and the federal government. The content is tailored for each of the CIKR sectors.

---

Safety Review Board, and The Infrastructure Security Partnership for review and comment.<sup>26</sup>

SSAs also offered other comments on their efforts to address changes to the NIPP—including changes to regional planning and risk management—in their SSPs. Five of the 18 officials representing different SSAs said that incorporation of these topics would not be difficult. For example, officials representing the Chemical, Dam, and the Emergency Services sectors SSAs said they did not foresee difficulty incorporating the key focus areas from the 2009 NIPP into their 2010 SSP rewrite. Representatives of the Commercial Facilities and Critical Manufacturing sectors said that they found the DHS guidance useful to their SSPs. The Water sector representative discussed programs or activities that were ongoing or planned that addressed each of the topics. For example, the Water sector SSA representative said the Environmental Protection Agency, which is the Water sector SSA, is working with DHS and other security partners to ensure risk assessment methodologies are upgraded and refined to be consistent with the NIPP to produce an analysis of risk that is consistent within the sector. Officials representing the Banking and Finance and Defense Industrial Base SSAs said it was premature to discuss how the changes related to risk management, regional coordination, performance measurement, and cyber security and international interdependencies would affect their agencies' efforts as the revision process was ongoing. The SSA official representing both the Postal and Shipping sector and the Transportation sector said that each change in the 2009 NIPP would be addressed according to its unique characteristics for the sectors.<sup>27</sup>

---

<sup>26</sup>The American Society of Civil Engineers represents more than 147,000 members of the civil engineering profession—the construction of roads, bridges, and other infrastructure for public use—worldwide. The National Dam Safety Review Board provides the Director of FEMA with advice in setting national dam safety priorities and considers the effects of national policy issues affecting dam safety. The Infrastructure Security Partnership is a nonprofit partnership to be a national asset facilitating dialogue on domestic infrastructure security, offering sources of technical support and sources for comment on public policy related to the security of the nation's built environment.

<sup>27</sup>As shown in table 1, the SSA for the Transportation and the Postal and Shipping sectors is the Transportation Security Administration.

---

## DHS Increased Its Emphasis on Resiliency in the 2009 NIPP and Directed SSAs to Address Resiliency in Their Sector Plans

Although DHS revised the NIPP to increase the use of the term resilience and to highlight it as an important concept paired with protection, the 2009 NIPP uses much of the same language as the 2006 NIPP to describe resiliency concepts and strategies. According to NIPP PMO officials, the 2009 NIPP has been updated to recognize the importance of resiliency and provide SSAs the requested flexibility to incorporate resiliency within the context of their sectors.

---

## DHS Increased Its Emphasis on Resiliency in the 2009 NIPP, but Used Much of the Same Language as in the 2006 NIPP

DHS increased its emphasis on resiliency in the 2009 NIPP by using the term more frequently and generally treating it as a concept formally paired with protection. Specifically, the 2006 NIPP used resiliency or resiliency-related terms 93 times while the 2009 NIPP used resiliency-related terms 183 times, about twice as often.<sup>28</sup> More importantly, whereas the 2006 NIPP primarily treated resiliency as a subset of protection, the 2009 NIPP generally referred to resiliency alongside protection. Both the 2006 and 2009 NIPPs include building resilience in the definition of protection, but the 2009 NIPP increased the profile of resilience by treating it as separate but related to CIKR protection. For example, whereas the Managing Risk chapter of the 2006 NIPP has a section entitled “Characteristics of Effective Protection Programs,” the same chapter in the 2009 NIPP has a section entitled, “Characteristics of Effective Protection Programs and Resiliency Strategies.”

In addition, in contrast to the 2006 NIPP, the 2009 NIPP referred to resiliency alongside protection in the introductory section of the document. Whereas the introduction to the 2006 NIPP states that it “...provides the mechanisms for...enhancing information-sharing mechanisms and protective measures within and across CI/KR sectors...,” the introduction to the 2009 NIPP states that it “...provides the mechanisms for...enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors.” Also, in comparison to the 2006 NIPP, the 2009 version of the NIPP discusses resiliency more often in the “Authorities, Roles and Responsibilities”

---

<sup>28</sup> As noted earlier, we counted the following resiliency-related terms—resilience, resiliency, resilient, and continuity (business continuity or operational continuity).

---

chapter of the document. These differences include a discussion on the expanded roles and responsibilities of key partners, such as SSAs and state and local governments, in CIKR planning with regard to resiliency. In this section of the 2006 NIPP, resiliency was discussed almost exclusively with regard to private sector owners and operators. NIPP PMO officials told us they wanted to recognize resilience as an approach to risk management, but some security partners did not see how they could or should influence the resilience efforts of the private sector. These PMO officials said with the release of the 2009 NIPP, they made a more concerted effort to help security partners understand how they can promote both protection and resilience.

NIPP PMO officials told us that changes related to resiliency in the 2009 NIPP were not intended to represent a major shift in policy; rather they were intended to increase attention to and raise awareness about resiliency as it applies within individual sectors. These officials told us that the concept of resiliency was always included in the NIPP. The 2006 NIPP addressed resilience and even talked about it being one way to enhance protection. However, NIPP PMO officials said that many partners interpret or use protection as synonymous with physical protection. To ensure that all NIPP partners properly understand the intent of the NIPP, the NIPP PMO has more explicitly addressed the concept of resiliency in the 2009 NIPP. These officials said that this more explicit emphasis on resilience in the 2009 NIPP is expected to encourage more system-based sector and cross-sector activities that address a broader spectrum of risks. This would include, for example, increased attention to cyber security—which can transcend different sectors—and discussion of the importance of systems and networks within and among sectors as a means of fostering resilience.

NIPP PMO officials also told us that the 2006 edition of the NIPP was developed based on the requirements of HSPD-7, which did not include an explicit emphasis on resiliency. They said that the 2009 NIPP was developed taking into account concerns raised by stakeholders that the 2006 NIPP emphasized asset protection rather than resiliency. They explained that, shortly after the 2006 NIPP was released, as the NIPP risk management framework and the sector partnerships matured, some stakeholders believed that the concept of continuity and resilience in and of itself, was not articulated and addressed as clearly as needed for their purposes. In addition, according to these officials, changes in the 2009 NIPP were drawn from many sources, including members of Congress and academic and policy groups, who also expressed increasing interest in the concept of resiliency as a critical part of national preparedness.

---

## DHS Is Encouraging SSAs to Emphasize Resiliency in Their 2010 SSPs

Although DHS provides SSAs flexibility when developing their SSPs, given increased attention to resiliency in the 2009 NIPP, NIPP PMO officials have encouraged SSAs to emphasize resiliency in guidance provided to SSAs in updating SSPs. One key difference between the guidance for developing the 2007 SSPs and the 2010 SSPs is the inclusion of a resiliency term in many places where there is a reference to protection or protection programs. For instance, Chapter 5 of the 2006 guidance is entitled “Develop and Implement Protective Programs.” By contrast, chapter 5 of the 2009 guidance is entitled “Develop and Implement Protective Programs and Resiliency Strategies.” Related to this change, DHS has also included instructions for where—and at times, how—resiliency is to be incorporated into 2010 SSPs. For example, in the 2009 guidance set forth in Chapter 5, SSAs are advised that in sectors for which infrastructure resiliency is as or more important than physical security or hardening, their SSA chapter on “Protection Program Implementation” should focus on describing the resiliency measures and strategies being used by the sector.<sup>29</sup> The guidance also provided examples of resiliency measures such as building hazard resistance into initial facility design; designing and developing self-healing and self-diagnosing cyber systems; and incorporating smart materials and embedded sensors into new physical and cyber networks.<sup>30</sup> According to DHS officials in the NIPP PMO, greater attention to interdependencies and cyber security in the NIPP are resiliency-related considerations that reinforce the need for SSAs to address systems- and network-based CIKR.

We did not examine the 2010 SSPs to determine the extent to which they adhered to DHS’s recent SSP guidance because SSPs were not complete at the time of our review. However, we examined the 2007 SSPs prepared based on 2006 guidance to ascertain the extent to which they contained language about resiliency. Our review showed that 13 of the 17 SSPs used the term resiliency or terms related to resiliency, such as continuity of operations, in their vision statements, goals, or objectives and 14 of 17 included resiliency in their risk management discussions. Whereas the

---

<sup>29</sup>The term “hardening” refers to making physical changes to a facility or creating additional redundancies to enhance its protection.

<sup>30</sup>DHS has also made commensurate changes to its 2009 SAR guidance. For example, the 2009 SAR guidance directs the SSAs to address resiliency in most sections of their annual reports. In addition, SSAs are asked to consider whether efforts to improve resiliency for the sector should be considered as part of changes in policy, resources, personnel, and facilities and states that resiliency activities should be documented as part of the sector’s path forward.

---

discussion of resiliency in the risk management section was relatively limited in some SSPs, the discussion about resiliency in others—particularly the banking and finance, energy, communications, and postal and shipping and transportation sectors—was relatively extensive. For example, the 2007 National Monuments SSP mentions resiliency in the Introduction, in reference to national goals and in a discussion about the importance CIKR protection has in making the nation more resilient. On the other hand, the Banking and Finance and Communications SSPs discuss how resilient these sectors are by design. For example:

- **Banking and Finance Sector:** The sector consists of many thousands of depository institutions, securities and futures firms, insurance companies, and other financial service companies, and supports a number of exchanges and over-the-counter markets, all of which contribute to the sector's resiliency because they provide a high degree of redundancy across the sector. Thus, according to the SSP, the competitive structure of the financial industry and the breadth of the financial instruments provide a level of resiliency against attack and other types of physical or cyber disruptions. The Banking and Finance SSP goes further by listing publications related to resiliency and business continuity planning and notes the Department of the Treasury encourages security partners to develop, enhance, and test business continuity plans. The SSP states that these plans are designed to preemptively identify the core functions and capabilities necessary to continue operations or resume operations after a disruption. The Banking and Finance SSP also notes that there is an annual test of business continuity planning by some members of the sector.
- **Communications Sector:** Resiliency is achieved by the technology, redundancy, and diversity employed in network design and by customers who employ diverse and resilient primary and backup communications capabilities, thereby increasing the availability of service to customers and reducing the impact of outages. For example, according to the Communications SSP, the network backbone remained intact on September 11, 2001, and during the hurricanes of 2005 despite the enormity of these incidents.

We interviewed SSA representatives about the extent to which they had included a discussion of resiliency in their past SSPs, and their plans to expand on their discussion of resiliency in their 2010 SSPs. Seventeen of the 18 SSA representatives who responded to our questions told us they believe that they have already included the concept of resiliency in their existing sector plans, although that term itself may not have been used often. These SSA representatives also said that they intend to further

---

incorporate resiliency into their 2010 SSPs where appropriate based on the characteristics of their sectors and their understanding of DHS guidance. However, based on their comments, it is likely that SSAs will not make significant changes to their SSPs with regard to resiliency. For example:

- **Banking and Finance Sector:** The SSA representative said they are reviewing the DHS guidance and working with DHS to coordinate perspectives regarding resiliency and to ensure that it remains central to their efforts regarding infrastructure issues. The Banking and Finance SSA representative added that inasmuch as the Department of the Treasury has long focused on the issue of resilience within the financial services sector, any changes to the Banking and Finance SSP concerning resiliency would be modest.
- **Chemical Sector:** The SSA representative said the sector has long recognized that “resilient operations and effective loss prevention are a part of managing risk. These concepts, when woven together, support the umbrella of resiliency.” The SSA representative said that resiliency, in terms of prevention, protection, response, and recovery along the preparedness spectrum was covered in the 2007 SSP and the SSA anticipates highlighting and framing the discussion of these items in terms of resiliency in the 2010 SSP update.
- **Nuclear Sector:** The SSA representative responded that, while resiliency is an important goal for some aspects of the Nuclear Sector, most Nuclear Sector programs focus on protection—physical hardening, in addition to other protective strategies—as the underlying goal because of the relatively serious consequences of a successful attack on some nuclear sites. According to the SSA representative, the draft 2010 Nuclear SSP highlights those areas where resilience is most appropriate, while retaining the overall focus on protection.

Finally, the SSA representative (a DHS TSA official) for the Transportation and Postal and Shipping sectors said he did not think that DHS merely wanted the SSAs to substitute the term resiliency where the existing plan said “redundancy” or “recovery” and would need to clarify the issue with DHS. For a discussion of resiliency in the SSPs, see appendix II.

DHS officials in the NIPP PMO told us that the balance between protection and resilience is unique to each sector and it must be recognized that the degree to which any one SSP increases the emphasis on resiliency will depend on the nature of the sector and the risks to its CIKR. They also said they will rely on the sectors themselves to determine the importance of resiliency in their plans. NIPP PMO officials further stated that by

---

emphasizing both protection and resilience in the NIPP, the private sector better appreciates that the NIPP gives them the flexibility to take actions and implement strategies that are tailored to their risks and situation. DHS officials said that they plan to provide additional guidance or instruction regarding resiliency to any sectors that need additional clarification, and, expect it to take time for resiliency to be fully understood and incorporated across the sectors.

---

## Agency Comments

We requested comments on a draft of this report from the Secretary of Homeland Security. In commenting on this draft DHS reiterated that it incorporated changes into the NIPP that reflect stakeholder input and the sectors' experience in protecting critical infrastructure. In addition, DHS said it increased the emphasis on resilience in the 2009 NIPP and directed SSAs to address resilience in the revision of their SSPs. DHS said the changes related to resilience in the 2009 NIPP were not intended to represent a major shift in policy as the concept of resilience was included in the 2006 NIPP. DHS said that the more explicit emphasis on resilience in the 2009 NIPP is expected to encourage more system-based sector and cross-sector activities that address a broader spectrum of risks. DHS also provided technical comments that we have incorporated as appropriate.

We also provided a draft of this report to SSAs representatives at the Departments of Agriculture, Defense, Energy, Health and Human Services, Interior, and Treasury and the Environmental Protection Agency and asked them to comment on those areas of the report relevant to their agencies. DOD, Health and Human Services and the Environmental Protection Agency provided technical comments that we have incorporated where 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, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

---

If you or your staff has any questions about this report or wish to discuss the matter further, please contact me at (202) 512-8777 or [caldwells@gao.gov](mailto:caldwells@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix IV.

A handwritten signature in black ink, appearing to read "Stephen Caldwell", with a checkmark at the end.

Stephen L. Caldwell  
Director, Homeland Security and Justice Issues

---

# Appendix I: The Concept of Resiliency

---

This appendix discusses how resiliency has been addressed in the context of critical infrastructure and key resource (CIKR) protection since 2006. The concept of resiliency has gained particular importance and application in a number of areas of federal CIKR planning. Both members of Congress and executive branch agencies have addressed resiliency in relation to the importance of the recovery of the nation's critical infrastructure from damage. Accordingly, most of the current focus is on assets, systems, and networks rather than agencies or organizations.

Part of the recent discussion over resiliency has focused on the definition of the concept. In February 2006, the Report of the Critical Infrastructure Task Force of the Homeland Security Advisory Council defined resiliency as “the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.” Later in 2006, the Department of Homeland Security’s National Infrastructure Protection Plan—again focusing on critical infrastructure, not agencies—defined resilience as “the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident.” In May 2008, the House Committee on Homeland Security held a series of hearings focusing on resilience at which government and private sector representatives, while agreeing on the importance of the concept, presented a variety of definitions and interpretations of resilience. Also, in April 2009, we reported that organizational resiliency is based on 21 attributes particularly associated with resilience and assigned them to five related categories. These categories are emergency planning, organizational flexibility, leadership, workforce commitment, and networked organizations.<sup>1</sup> Likewise, government and academic organizations have discussed how resiliency can be achieved in different ways. Among these are an organization’s robustness (based on protection, for example better security or the hardening of facilities); the redundancy of primary systems (backups and overlap offering alternatives if one system is damaged or destroyed); and the degree to which flexibility can be built into the organization’s culture (to include continuous communications to assure awareness during a disruption, distributed decision-making power so multiple employees can take decisive action when needed, and being conditioned for disruptions to improve response when necessary).

---

<sup>1</sup>See *IRS Management: IRS Practices Contribute to Its Resilience, but Would Benefit from Additional Emergency Planning Efforts*, [GAO-09-418](#) (Washington, D.C.: Apr. 9, 2009).

The concepts associated with resiliency, and related concepts—e.g., recovery and reconstitution and continuity of operations—have evolved over the years. Homeland Security Presidential Directive-7 did not contain specific references to resiliency, but it provided instructions to federal agencies to create protection plans for the facilities they own and operate to include “...contingency planning, including the recovery and reconstitution of essential capabilities.” Also, in May 2007 the President issued Homeland Security Presidential Directive 20 - *National Continuity Policy*. This directive establishes a comprehensive national policy on the continuity of federal government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of federal continuity policies. It also establishes "National Essential Functions," directs executive departments and agencies to integrate continuity requirements into operations, and provides guidance for state, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that is to enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency. As part of Homeland Security Presidential Directive 20, the Secretary of Homeland Security is directed to, among other things, coordinate the implementation, execution, and assessment of continuity operations and activities; develop, lead, and conduct a federal continuity training and exercise program, which shall be incorporated into the National Exercise Program; and develop and promulgate continuity planning guidance to state, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators.

In August 2009 the Homeland Security Studies and Analysis Institute released a report that examined the operational framework that could be used by DHS and stakeholders at all levels, both public and private, as a basis for incorporating resilience into our infrastructure and society in order to make the nation safer.<sup>2</sup> This framework approached resilience in terms of three mutually reinforcing objectives: resistance, absorption, and restoration.

- *Resistance* is accomplished when the threat or hazard damage potential is limited through interdiction, redirection, avoidance, or

---

<sup>2</sup>The Homeland Security Studies and Analysis Institute, *Concept Development: An Operational Framework for Resilience* (Aug. 27, 2009).

neutralization efforts. The entire system experiences less damage than would otherwise be the case.

- *Absorption* is accomplished when consequences of a damage-causing event are mitigated. The system experiences damage, but maintains its structure and key functions. It bends, but does not break.
- *Restoration* is accomplished when the system is rapidly reconstituted and reset to its present status. Key functions are reestablished, possibly at alternative sites or with substitute processes, and possibly at an enhanced level of functionality.

Finally, the study includes funding profiles for the resistance, absorption, and restoration objectives dependent upon whether the facility or entity wants to put an emphasis on avoiding damage up front (protection) or the ability to recover from damage quickly.

Most recently, the National Infrastructure Advisory Council issued a report on critical infrastructure resilience in September 2009.<sup>3</sup> The study noted that protection and resilience are not opposing concepts and represent complementary and necessary elements of a comprehensive risk management strategy. It examined current government policies and programs for resilience in CIKR sectors. It also focused on identifying measures to achieve sector- and national-level resilience, cross-sector and supply-chain-related issues as they relate to resilience, and measures implemented by individual enterprises. The NIAC made resilience-related recommendations to the President through the DHS Secretary to improve government coordination, clarify roles and responsibilities, and strengthen public-private partnerships and to encourage resilience using market incentives.

---

<sup>3</sup>The National Infrastructure Advisory Council (NIAC) is primarily composed of private sector CIKR representatives and provides the President with advice on the security of the 18 Critical Infrastructure and Key Resource (CIKR) sectors and their information systems. The NIAC also advises the lead federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. The NIAC report, *Critical Infrastructure Resilience: Final Report and Recommendations*, was published September 8, 2009.

---

# Appendix II: Discussions of Resiliency in 2007 Sector-specific Plans

---

This appendix discusses how the Sector-specific Agencies (SSAs) addressed resiliency in their 2007 Sector-specific Plans (SSPs) and how the SSAs will address resiliency in their 2010 SSPs. All 17 SSAs in place at the time the 2007 SSPs were developed incorporated resiliency-related terms—resilient, resilience, resiliency, and continuity planning—into their 2007 SSPs.<sup>1</sup> Specifically, 13 of the 17 SSPs used these terms in their vision statements, goals or objectives, and 14 of the 17 used these terms in their risk management plans.

Given the increased attention to resiliency in the 2009 National Infrastructure Protection Plan (NIPP) NIPP, NIPP Program Management Office (PMO) officials encouraged SSAs to devote more attention to resiliency in their 2010 SSPs. Since the Department of Homeland Security (DHS) does not expect these plans to be released until 2010, we contacted representatives of the 18 SSAs<sup>2</sup> to gather information on their plans to adhere to DHS's revised SSP guidance. Representatives of 7 of the 18 sectors—Agriculture and Food, Communications, Government Facilities, Healthcare and Public Health, Information Technology (IT), Postal and Shipping, and Transportation—responded that they intend to devote greater attention to resiliency, and representatives of 10 of the 18 sectors—Banking and Finance, Chemical, Commercial Facilities, Dams, Defense Industrial Base, Emergency Services, Energy, National Monuments, Nuclear, and Water—responded that they intend to devote the same amount of attention to resiliency as in their 2007 SSPs. Finally, a representative of 1 of the 18 sectors—Critical Manufacturing—responded that the sector's first SSP, to be released in 2010, will describe the sector's strategy to increase resiliency and prevent, deter, and mitigate any disruptions caused by man-made threats or natural disasters.

The following table gives an overview of how resilience was referenced in the 2007 SSPs and how sector representatives stated they will address resiliency in their 2010 SSPs.

---

<sup>1</sup>We limited our analysis to how often and where resiliency-related terms—resiliency, resilience, resilient, and continuity—were used in these plans. In commenting on our approach, DHS said this was a reasonable set of terms for our analysis.

<sup>2</sup>DHS designated Critical Manufacturing as the 18<sup>th</sup> CIKR sector in March 2008.

**Appendix II: Discussions of Resiliency in 2007  
Sector-specific Plans**

**Table 3: Sector Plan References to Resiliency**

<b>Sector</b>	<b>Resiliency overview</b>
Agriculture and Food	The 2007 Agriculture and Food SSP addressed resiliency as a component of protection. For example, the Introduction noted that protecting the Nation's Critical Infrastructure and Key Resources (CIKR) makes the United States more resilient to terrorist attacks and natural and man-made disasters. A sector representative stated that the sector will integrate the concepts of resiliency and protection in its 2010 SSP.
Banking and Finance	The 2007 Banking and Finance SSP extensively addressed resiliency. For example, the plan noted that resiliency is built into sector risk management activities, which include prioritization, participation in regional and national exercises, research and development, and training. In addition, the plan noted that the Treasury Department, the sector's SSA, encourages security partners to develop business continuity plans, and determines the success of the annual, industrywide business continuity planning test. A sector representative stated that only modest changes to the 2010 plan are foreseen because the sector already focuses heavily on resilience.
Chemical	The 2007 Chemical SSP addressed resiliency as a component of protection. For example, the plan noted that protection can include a wide range of activities, such as building resiliency and redundancy. A sector representative said that while resilience was covered in the 2007 SSP's discussion of preparedness, the 2010 SSP will reframe the discussion to highlight the term resiliency.
Commercial Facilities	The 2007 Commercial Facilities SSP addressed resiliency by focusing on continuity planning. Specifically, the plan noted: (1) business continuity plans are often included in the public sector's risk management processes; (2) state, local, and tribal governments are responsible for the continuity of essential services at commercial facilities under their jurisdiction; and (3) the owner of a facility is responsible for the continuity of critical functions. A sector representative noted that the sector has always stressed the need to return to normalcy as quickly as possible after a disaster.
Communications	The 2007 Communications SSP extensively addressed resiliency. For example, the plan discussed how the sector mitigates cascading effects of incidents by building resilient communications systems and networks to ensure disruptions remain largely localized and do not affect the national communications backbone. According to a sector representative, the 2010 plan is expected to provide a description of the sector's resiliency activities and explain how government and industry are to work together to overcome emerging challenges and impediments to risk reduction.
Critical Manufacturing	The Critical Manufacturing sector was established in 2008; therefore, it did not release a 2007 SSP. According to a sector representative, the sector intends to issue a 2010 SSP, which will explain the sector's strategy to increase resiliency and prevent, deter, and mitigate any disruptions caused by man-made threats or natural disasters.
Dams	The 2007 Dams SSP addressed resiliency as a component of protection. For example, the Introduction noted that protecting the nation's CIKR makes the United States more resilient to terrorist attacks and natural and man-made disasters. A sector representative said resiliency, which the sector defines as "contingency planning in the form of emergency action plans, response plans, security plans and continuity of operations plans," has always been and will continue to be incorporated into sector planning efforts, including the 2010 SSP.
Defense Industrial Base	The 2007 Defense Industrial Base (DIB) SSP addressed resiliency. For example, the plan noted one of its goals was to reduce the number of critical DIB assets whenever and wherever possible within fiscal and legal constraints. A sector representative said that the 2010 SSP will devote the same amount of attention to resiliency as in the 2007 SSP.

**Appendix II: Discussions of Resiliency in 2007  
Sector-specific Plans**

<b>Sector</b>	<b>Resiliency overview</b>
Emergency Services	The 2007 Emergency Services SSP addressed resiliency as a component of protection. For example, the plan stated that protection makes CIKR more resilient, and protection includes building resiliency and redundancy. A sector representative did not foresee issues updating the 2010 SSP because resiliency is already a key feature in the Emergency Services sector.
Energy	The 2007 Energy SSP addressed resiliency. For example, the plan described the sector as resilient because electricity flows freely along all available alternating current paths in the network. These multiple paths provide resiliency to instantly respond to both planned and unexpected equipment outages in the system. A sector representative noted that the energy sector has always embraced the necessity of resiliency and is engaged in a variety of resiliency-related projects dealing with continuity of business planning.
Government Facilities	The 2007 Government Facilities SSP addressed resiliency by focusing on continuity of government operations, particularly in regard to planning, coordination and information sharing. For example, the plan identified coordination, mechanisms and recommended continuity actions that facilities can take to ensure the continuity of essential operations, functions, and services. According to a sector representative, the sector's focus on resilience has been reinforced with the release of Homeland Security Presidential Directive (HSPD) 20 and other federal directives. <sup>3</sup> These new policy frameworks have been used to enhance exercise programs that focus on the continuity of government operations, leading to a more resilient framework for the sector.
Healthcare and Public Health	The Healthcare and Public Health SSP addressed resiliency. For example, in an emergency, healthcare capabilities are to be coordinated within the sector to ensure resiliency across other CIKR sectors because these sectors rely on the healthcare sector for their resiliency. According to an SSA representative, the 2010 SSP will be more in-depth than the 2007 SSP in certain sections. For example, the 2010 SSP will focus on workforce and supply network resiliency because the Healthcare and Public Health sector is generally made up of systems and networks.
Information Technology	The 2007 Information Technology (IT) SSP addressed resiliency. For example, the plan said that critical functions must be resilient to threats, and the ability to respond to crises promotes resilience. The plan also noted that resources are needed to improve IT resilience and the National Cyber Security Division must be ready with resources to contribute to improving resilience when security investments are beyond the capability of the private sector. According to a sector representative, the 2010 SSP is expected to outline the sector's concept of resiliency by describing the sector's risk management framework, which involves assessing risk, prioritizing risk mitigation strategies, and informing sector protective programs, research and development efforts. The representative expects these activities will increase the resiliency of IT sector functions.
National Monuments	The 2007 National Monuments SSP addressed resiliency as a component of protection. For example, the plan noted that protection can include a wide range of activities, including building resiliency and redundancy. A sector representative noted that changes to the 2009 NIPP will not have an impact upon the sector's 2010 SSP because the sector focuses more on protection than on resiliency.
Nuclear	The 2007 Nuclear SSP addressed resiliency as a component of protection. For example, the plan noted that resiliency planning should be recognized as part of protection planning. A sector representative said the draft 2010 SSP highlights areas where resilience is appropriate, but retains its overall focus on protection.

<sup>3</sup>See app. 1 for a more detailed discussion of HSPD-20.

---

**Appendix II: Discussions of Resiliency in 2007  
Sector-specific Plans**

<b>Sector</b>	<b>Resiliency overview</b>
Postal and Shipping	The 2007 Postal and Shipping SSP addressed resiliency by focusing on continuity planning. For example, the plan noted sector continuity is important for daily economic and personal transactions, so assets and systems are designed to ensure business continuity even if individual assets are unable to provide services. For the 2010 SSP, a sector representative said the sector needs to broaden its risk mitigation activities by developing resiliency targets and group resiliency programs to track how improving resiliency reduces risk.
Transportation	The 2007 Transportation SSP extensively addressed resiliency. For example, the plan discussed surface transportation, tunnel, freight, and pipeline programs that enhance the sector's resiliency. For the 2010 SSP, a sector representative said the sector needs to broaden its risk mitigation activities by developing resiliency targets and group resiliency programs to track how improving resiliency reduces risk.
Water	The 2007 Water SSP addressed resiliency. For example, the plan noted that research into architecture and systems design will focus on continuity of service and resiliency for the uninterrupted provision of safe water. A sector representative stated that the Environmental Protection Agency, the Sector's SSA, will continue to incorporate resilience into its 2010 SSP; therefore, major revisions related to resilience will not be necessary.

---

Source: 2007 SSPs and interviews with sector representatives.

# Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

February 25, 2010

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

Dear Mr. Caldwell:

Re: Draft Report GAO-10-296, Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience (GAO Job Code 440818)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's draft report referenced above. The report addresses (1) how the 2009 National Infrastructure Protection Plan (NIPP) changed compared to the 2006 NIPP and what process was used to identify and incorporate the changes; and (2) how have DHS and sector specific agencies (SSAs) addressed the concept of critical infrastructure resiliency as part of our national critical infrastructure and key resources (CIKR) and sector-specific planning efforts. These questions have largely been addressed by summarizing and documenting DHS's approach to develop the 2009 NIPP and the related efforts by DHS and the SSAs to develop the 2010 Sector-Specific Plans (SSPs) that support the NIPP. The report contains no recommendations and DHS appreciates the recognition of efforts taken with respect to resiliency.

As noted in the draft report, DHS incorporated changes into the NIPP that reflect stakeholder input and the sectors' experience in protecting critical infrastructure. In addition, DHS increased the emphasis on resilience in the 2009 NIPP and directed SSAs to address resilience in the revision of their SSPs. Changes related to resilience in the 2009 NIPP were not intended to represent a major shift in policy; rather they were intended to increase attention to and raise awareness about resilience as it applies within individual sectors. The concept of resilience was included in the 2006 NIPP as one of many different ways to enhance protection. However, by not seeing resilience strategies in places where protective programs were mentioned, some of the sector partners thought that approaching risk management through increased resilience was not explicitly accepted and promoted under the NIPP. The more explicit emphasis on resilience in the 2009 NIPP is expected to encourage more system-based sector and cross-sector activities that address a broader spectrum of risks.

Sincerely,

A handwritten signature in black ink that reads "Jerald E. Levine".

Jerald E. Levine  
Director  
Departmental GAO/OIG Audit Liaison Office

---

# Appendix IV: GAO Contacts and Acknowledgments

---

## GAO Contact

Stephen L. Caldwell (202) 512-8777

---

## Acknowledgments

In addition to the contact named above, John Mortin, Assistant Director and Tony DeFrank, Analyst-in-Charge, managed this assignment with assistance from Christy Bilardo and Landis Lindsey. Michele Fejar and Steven Putansu assisted with design and methodology. Tracey King and Thomas Lombardi provided legal support and Lara Kaskie provided assistance in report preparation.

---

# GAO Products Related to Critical Infrastructure Protection

---

## Critical Infrastructure Protection

*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 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](#). Washington, D.C.: 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: 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](http://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](http://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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto: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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

