



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 19, 2011

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

The Honorable Sheila Jackson-Lee
Ranking Member
Subcommittee on Transportation Security
House of Representatives

Subject: *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*

This letter formally transmits the enclosed briefing in response to your request to review the Department of Homeland Security's framework¹ for securing critical infrastructure and key resources (CIKR),² and subsequent agency comments. As such, this correspondence provides information on: (1) how DHS coordinates with CIKR stakeholders to identify overlaps and gaps in CIKR security activities across all sectors,³ (2) how DHS addresses these potential overlaps in CIKR security activities, and (3) how DHS addresses CIKR security gaps. To conduct this work, among other things, we selected a non-random sample of nine sectors with a mix of regulations related to security to obtain stakeholders views on working with DHS to identify and address overlaps and gaps in CIKR activities; reviewed applicable laws and regulations, DHS documents such as the National Infrastructure Protection Plan, and pertinent GAO reports; and interviewed DHS officials in the Office of Infrastructure

¹ The National Infrastructure Protection Plan (NIPP) is the national plan for coordinating the protection of the nation's critical infrastructure. For the purposes of this briefing, the framework also includes applicable regulations and security practices developed and/or adopted by CIKR stakeholders, such as federal, state, or local governments or industry trade associations.

² Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. Key resources are resources essential to the minimal operations of the economy and government.

³ Consistent with the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, as amended, and Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003), DHS uses a voluntary public-private partnership approach, as appropriate, to enhance the protection of the CIKR. There are 18 CIKR sectors, each of which is assigned a sector-specific agency (SSA). SSAs are federal agencies responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

Protection (IP) in the National Protection and Programs Directorate and officials representing the sectors we selected. While the results of these efforts are not generalizable to all CIKR sectors, stakeholders, and activities, they provided valuable insights into CIKR partner perspectives across a range of CIKR.

In summary we found:

- DHS coordinates with CIKR stakeholders, including other federal regulatory authorities, through information-sharing mechanisms, such as council meetings, and other efforts to identify overlaps and gaps in CIKR security activities.
- DHS is taking action to address overlapping security activities by clarifying roles and responsibilities for CIKR security activities with agencies that have regulatory oversight, such as the Nuclear Regulatory Commission, through coordination mechanisms, including memorandums of understanding and working groups.
- DHS works to address gaps in infrastructure security by developing and distributing tools such as guides that promote common security activities; conducting voluntary training and security exercises to enhance security capabilities; providing information on resources available to security partners; and, as appropriate, conducting site vulnerability assessments and security surveys at both public and privately owned facilities that voluntarily participate in such efforts.

For additional information on the results of our work, please see enclosure I, the briefing we provided your offices on May 12, 2011. We are not making any recommendations for congressional consideration or agency action.

In commenting on a draft of this report, DHS agreed with the report's findings. DHS's comments are reprinted in enclosure II. DHS also provided technical comments on the enclosed briefing, which we incorporated as appropriate.

This concludes the first phase of our work on CIKR security activities. As agreed with your offices, we will continue our work in this area by reviewing DHS's voluntary programs and its efforts to measure the effectiveness of these programs. We will report the results in 2012.

Also, unless you publicly announce the contents of this correspondence earlier, we plan no further distribution until 30 days from the correspondence's date. At that time, we will send copies of the correspondence to interested congressional committees and other interested parties. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>. Should you or your staff have questions concerning this report or wish to discuss the matter further, please contact me at (202) 512-8777 or caldwells@gao.gov. Contact points for our Offices of

Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were John Mortin, Assistant Director; Labony Chakraborty; Andrew Curry; Tony DeFrank; Michele Fejfar; Thomas Lombardi; Kendal Robinson; and Luis Rodriguez.

A handwritten signature in black ink, appearing to read "Steve Caldwell". The signature is fluid and cursive, with a large initial "S" and a checkmark-like flourish at the end.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Enclosures (2)

Enclosure I

Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities



Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities

Briefing to Congressional Requesters
May 12, 2011

Page 1

Overview

Introduction

Objectives

Scope and Methodology

Results in Brief

Background

Findings

Agency Comments

Related GAO Products

Introduction

- The protection and resilience of the critical infrastructure in the United States is essential to the Nation's security, maintaining public health and safety, and promoting the Nation's economic vitality. The Department of Homeland Security (DHS), as appropriate, uses a voluntary public-private partnership approach to enhance the protection of the nation's critical infrastructure and key resources (CIKR).¹
- There are 18 CIKR sectors—such as Chemical, Transportation, and Energy—each having a Sector Specific Agency (SSA). SSAs are the federal agencies responsible for coordinating CIKR protection efforts with the public and private stakeholders in their respective sectors.

¹ Consistent with the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, as amended, and Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003), DHS uses a voluntary public-private partnership approach, as appropriate, to enhance the protection of the CIKR. Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security while key resources are resources essential to the minimal operations of the economy and government. See Pub. L. No. 107-296, § 2(4), (9), 116 Stat. at 2140-41, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 400-02 (codified at 42 U.S.C. § 5195c), and HSPD-7, § 6(a), (b).

Introduction (continued)

- Within DHS, the Office of Infrastructure Protection (IP) in the National Protection and Programs Directorate (NPPD) is responsible for CIKR protection. While other entities may possess and exercise regulatory authority over CIKR to address security,² IP generally relies on voluntary efforts to secure CIKR due to its limited authority to directly regulate most CIKR. In this role, IP coordinates with CIKR stakeholders including other federal agencies, state and local government agencies and authorities, the private sector, and other entities, such as the Federal Senior Leadership Council, which is made up of federal agencies with a role in implementing CIKR security.

² For example, the Nuclear Regulatory Commission (NRC) regulates nuclear facilities.

Objectives

Members of Congress raised questions about potential overlaps and gaps³ in CIKR security measures. You requested that we review the DHS framework for securing CIKR.⁴ Therefore, our objectives were to identify actions DHS has taken to:

- (1) coordinate with CIKR stakeholders, including federal regulatory authorities, to identify overlaps and gaps in CIKR security activities;
- (2) address overlapping activities to improve coordination of CIKR security; and
- (3) address CIKR security gaps.

³ DHS uses the term "vulnerability" rather than "gaps" when referring to areas in need of improved security.

⁴ Our review did not focus on cybersecurity in critical infrastructure as this is addressed in other GAO work. For example: see GAO, *Information Technology: Federal Laws, Regulations, and Mandatory Standards to Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors*, GAO-08-1075R (Washington, D.C.: September 16, 2008).

Scope and Methodology

To conduct this work, we:

- reviewed applicable laws and regulations; DHS documents, such as the National Infrastructure Protection Plan (NIPP)—DHS’s national plan for coordinating the protection of the nation’s CIKR; and pertinent GAO reports;⁵
- selected a non-random sample of nine sectors with a mix of regulations related to security to obtain stakeholders views on working with DHS to identify and address overlaps and gaps in CIKR security activities—we also selected sectors where DHS IP, other DHS components and non-DHS agencies are the sector SSA. The results are not generalizable but provided insights on SSA activities across a range of CIKR;⁶
- interviewed DHS officials in the Office of Infrastructure Protection in the NPPD, representatives from 9 of 18 SSAs from the sectors we selected to review, and representatives from the Federal Energy Regulatory Commission and the NRC as their activities related to sectors we selected to review;
- discussed the NIPP framework and CIKR regulations with three state homeland security offices (California, New Jersey, and Virginia). We selected these states because they have extensive CIKR and different levels of security regulation. The results of these discussions are not generalizable to all state homeland security offices but provided perspectives about the NIPP framework and CIKR regulations (at all levels of government) across a range of CIKR.

⁵ See the related products list on page 20 of this briefing.

⁶ We selected and met with representatives from the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, Energy, Nuclear, Transportation, and Water sectors—a sample with a mix of regulations related to security.

Scope and Methodology (Continued)

- We also met with officials from one private sector company and one industry trade association with activities related to our sample of SSAs, to understand whether overlapping activities hinder the NIPP framework. The results are not generalizable, but provided insights on some industry perspectives.

To ensure the accuracy of the information in these slides, we obtained formal agency comments on the contents of this briefing.

We conducted this performance audit from August 2010 through May 2011⁷ in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

⁷ This concludes the first phase of our work. As agreed with your offices, we will continue our work in this area with a review of DHS's voluntary programs and its efforts to measure the effectiveness of these programs and will report the final results in 2012.

Results in Brief

- DHS coordinates with CIKR stakeholders, including other federal regulatory authorities, through information-sharing mechanisms, such as council meetings, and other efforts to identify overlaps and gaps in CIKR security activities.
- DHS is taking action to address overlapping security activities by clarifying roles and responsibilities for CIKR security activities with agencies that have regulatory oversight such as the NRC through coordination mechanisms, including Memoranda of Understanding and working groups.
- DHS works to address gaps in infrastructure security by developing and distributing security tools, such as guides that promote common security activities; conducting voluntary training and security exercises to enhance security capabilities; providing information on resources available to security partners; and by conducting site vulnerability assessments and security surveys at both public and privately-owned facilities that voluntarily participate in such efforts.

Background

- The Homeland Security Act of 2002 created DHS and gave the department wide-ranging responsibilities for, among other things, leading and coordinating national CIKR protection efforts.⁸ For example, the act required DHS to (1) develop a comprehensive national plan for securing the nation's CIKR and (2) recommend measures necessary 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.
- HSPD-7 further defined critical infrastructure protection responsibilities for DHS and SSAs. HSPD-7 directed DHS to, among other things, establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across CIKR sectors.⁹
- Table 1 reflects the SSAs responsible for coordinating CIKR protection efforts with the public and private stakeholders in these sectors.

⁸ See Pub. L. No. 107-296, § 201, 116 Stat. at 2145-46 (codified as amended at 6 U.S.C. § 121).

⁹ HSPD-7, § 14.

Background (continued)

Table 1: CIKR Sectors and SSAs

Sector-Specific Agency	CIKR Sector
Department of Agriculture	
Food and Drug Administration (HHS)	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
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
Department of Homeland Security	
<i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
<i>Office of Cybersecurity and Communications</i>	Communications Information Technology
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration and U.S. Coast Guard</i>	Transportation Systems Maritime Transportation Mode (subsector)
<i>Federal Protective Service</i>	Government Facilities
Department of Education	Educational Facilities (subsector)

Source: GAO analysis of 2009 National Infrastructure Protection Plan.

Background (continued)

- The National Infrastructure Protection Plan (NIPP) is the national plan for coordinating the protection of the nation's CIKR. First issued in 2006, and updated in 2009,¹⁰ the NIPP provides the overarching approach for integrating the nation's CIKR protection initiatives into a single national effort, sets forth a comprehensive risk management framework, and defines roles and responsibilities for infrastructure partners. The NIPP framework overlaps with existing security practices and federal and state laws and regulations.¹⁰
 - The NIPP reflects DHS's voluntary public-private partnership approach, and according to DHS, where appropriate, leverages existing regulatory frameworks. For example, according to agency officials, DHS recognizes that the commercial facilities and the critical manufacturing sectors may not be subject to federal or state laws and regulations related to security while there are a few sectors that are subject to specific security-related laws and regulations, such as the chemical, transportation, and nuclear sectors.¹¹

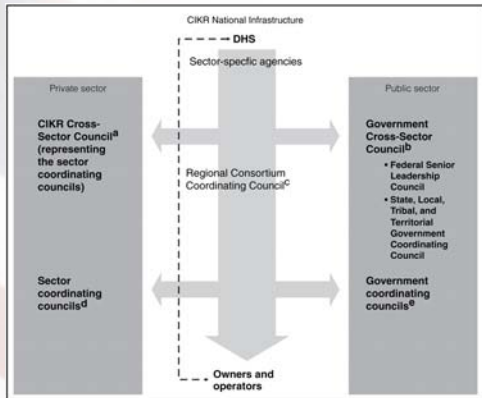
¹⁰ For the purposes of this briefing, a sector's security framework also includes laws, regulations, and security practices developed and adopted by sector stakeholders, such as federal and state governments, and industry trade associations.

¹¹ For example, the Chemical Facilities Anti-Terrorism Standards (CFATS), promulgated by DHS pursuant to the Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388-89 (2006), impose requirements on high risk chemical facilities in the U.S. to enhance the security of the United States by lowering the risk posed by those chemical facilities. See 67 Fed. Reg. 17,688 (Apr. 9, 2007) (codified as amended at 6 C.F.R. pt. 27). Consistent with the fiscal year 2007 DHS appropriations act, CFATS do not apply to facilities regulated pursuant to the Maritime Transportation Security Act (MTSA) of 2002, facilities owned or operated by the Departments of Defense or Energy, facilities subject to regulation by the NRC, and federally regulated public water systems and water treatment facilities.

Objective One: To Identify Infrastructure Security Overlaps and Gaps DHS Coordinates With CIKR Partners

- DHS leverages existing regulatory frameworks, where applicable, to implement the NIPP with its security partners within and across the 18 sectors and identify CIKR security overlaps and gaps to enhance and supplement existing sector regulations. To do so, DHS
 - coordinates through designated Federal government SSAs for each of the CIKR sectors to identify security overlaps and gaps as they implement the NIPP framework. For example, documents provided by one DHS SSA demonstrate how DHS coordinated with a federal regulator for the sector via official correspondence and urged consideration of the merits of both greater regulation and the enhancement of existing regulation to address security gaps and improve security in the sector;
 - coordinates with state officials with responsibility for CIKR efforts to facilitate the NIPP partnership. Officials with responsibility for CIKR efforts from three states, in addition to officials from the nine SSAs we visited, said that they had not identified state laws or regulations that overlap with or hinder the implementation of the NIPP; and
 - coordinates with other security partners to identify cross-sector overlaps and gaps through meetings with various councils including the Government Cross-Sector Council, the Federal Senior Leadership Council, the State, Local, Tribal, and Territorial Government Coordinating Council, and sector Government Coordinating Councils. (see figure 1)

Objective One: (continued)



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

- ^a Cross-sector issues and interdependencies are addressed among the Sector Coordinating Councils (SCCs) through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs.
- ^b Cross-sector issues and interdependencies between the Government Coordinating Councils (GCCs) will be addressed through the Government Cross-Sector Council, which comprises two sub-councils—the NIPP Federal Senior Leadership Council (NIPP FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The objective of the NIPP FSLC is to facilitate enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The SLTTGCC serves as a forum to ensure that state, local, and tribal homeland security partners are fully integrated as active participants in national CIKR protection efforts and to provide an organizational structure to coordinate across jurisdictions on state and local government-level CIKR protection guidance, strategies, and programs.
- ^c The Regional Consortium Coordinating Council (RCCC) brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among CIKR partners within and across geographical areas and sectors.
- ^d The Sector Coordinating Councils (SCCs) are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership will vary from sector to sector, reflecting the unique composition of each sector; however, membership should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector.
- ^e The Government Coordinating Council (GCC) comprises representatives from across various levels of government (Federal, state, local, or tribal), as appropriate to the operations of each individual sector.

- **Figure 1. CIKR Sector Partnership Model** illustrates the sector partnership model and the interrelationships among the various councils, sectors, and asset owners and operators.

Objective Two: To Address Overlaps in CIKR Security Activities DHS Works with Partners

- DHS is taking action to address overlapping security activities by clarifying roles and responsibilities for CIKR security activities and working with regulators to improve coordination of or harmonize CIKR activities. IP officials identified CFATS as the primary overlapping regulatory regime with potentially duplicative activities that they are addressing. Pursuant to the statute authorizing DHS to promulgate CFATS, certain facilities are not subject to CFATS, and DHS has taken additional actions to implement Memoranda of Understanding or Agreement to avoid overlap and duplication.
 - For example, at facilities where both CFATS and regulations implemented pursuant to MTSA may be applicable, two DHS components—NPPD and the U.S. Coast Guard—have been working together to clarify which facilities or parts of facilities are regulated by whom and avoid potentially overlapping efforts. In addition, there may be maritime facilities where part of the facility is subject to MTSA regulations while another part of the facility is subject to CFATS. According to officials from NPPD and the U.S. Coast Guard, the agencies established a joint CFATS-MTSA working group to review regulations across the two statutes, compare assessment efforts to secure the facilities, and where appropriate, implement methods to harmonize CFATS and MTSA regulations—through a joint action memo or other agreement. According to agency officials, efforts are also underway to examine the different treatment of regional planning efforts and cybersecurity requirements across the regulations. Coast Guard officials stated that they are currently developing timelines and specific action items for completing these efforts.

Objective Two: (continued)

- Where CFATS overlaps with NRC authority, DHS officials reported collaborating with NRC officials to clarify which facilities are regulated by whom and avoid overlapping efforts.
- Since CFATS took effect in 2007, IP has reduced some voluntary programs¹² on chemical facilities to avoid overlapping activities in the sector. For example, the number of voluntary site assessments conducted by IP on chemical facilities that voluntarily participated in the assessment decreased from nine to one assessment from 2008 to 2010.
- DHS officials also reported they have identified opportunities to collaborate with other federal agencies and evaluate how CFATS could apply to facilities or substances not currently subject to CFATS.
 - For example, DHS reported working closely with the Environmental Protection Agency to begin discussing how CFATS could be applied to water and wastewater treatment facilities, should they become subject to CFATS security regulations.
- According to DHS, DHS is also coordinating with Federal entities such as the Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Investigation; and U.S. Department of Agriculture to determine the best way to implement its regulatory authority over sales and transfers of ammonium nitrate.¹³ DHS officials stated that they are working to enhance the security of ammonium nitrate while avoiding placing any duplicative requirements on the regulated community.

¹² Voluntary programs, including these assessments, will be discussed in more detail later in this briefing.

¹³ See Dept of Homeland Security Appropriations Act, 2008, Pub. L. No. 110-161, Div. E, § 563, 121 Stat. 2042, 2083-90 (2007).

Objective Three: To Address Gaps in CIKR Security DHS Develops Resources and Conducts Voluntary Assessments

To address CIKR security gaps, DHS

- develops and distributes security tools, such as guides that promote common security activities; conducts voluntary training and security exercises to enhance security capabilities; and provides information on resources available to security partners from the 18 sectors through various efforts, including the Protective Security Advisor (PSA) Program. PSAs are DHS's protection specialists assigned as CIKR security coordinators between DHS and the protective community at the state, local, and private sector levels and are responsible for sharing risk information and coordinating DHS's voluntary programs:
 - For example, according to IP, in coordination with and at the request of the Director of Security, National Association for Stock Car Auto Racing (NASCAR), the SSA and NASCAR staff worked together to develop a security tool—a template and guidance for developing emergency response plans—for NASCAR events;
- conducts site vulnerability assessments and security surveys at and across facilities from the 18 sectors that voluntarily participate in these efforts, such as Site Assistance Visits (SAVs), and Enhanced Critical Infrastructure Protection (ECIP) security surveys, and uses these assessments to develop and disseminate information on steps owners and operators can take to protect their facilities to various stakeholders, generally on a need-to-know basis;
 - SAVs are facility vulnerability assessments that can last up to three days focused on identifying security gaps and providing options to enhance protective measures to CIKR owners and operators. According to DHS, DHS conducted 192 SAVs in fiscal year 2009 and 217 SAVs in fiscal year 2010;

Objective Three: (continued)

- ECIP security surveys are half-to-full day surveys conducted to assess overall facility security and increase security awareness. Protective measures are surveyed using a web-based Infrastructure Security Tool and presented to CIKR owners and operators in a way that allows them to see how their facility's security measures compare against similar facilities in the same sector or subsector. According to DHS, it conducted 989 ECIPs in fiscal year 2009 and 835 ECIPs in fiscal year 2010;
- According to DHS officials, the total number of SAVs and ECIPs both in the aggregate and by sector varies from year-to-year depending on the risk to facilities, state and local priorities, threat levels, DHS priorities, exercises, and the number and type of planned significant national events.¹⁴ In addition, since these efforts are voluntary, they depend on the interest and cooperation of facility owners and operators. Generally, however, in recent years, DHS has conducted fewer voluntary facility assessments on CIKR in sectors subject to more regulation, such as the chemical and nuclear sectors, and more activities in the commercial facilities sector, which is subject to less regulation;
- We are beginning additional work on DHS's voluntary programs and its efforts to measure the effectiveness of its voluntary programs in enhancing CIKR protection and resilience and will report the final results in 2012.

¹⁴ Significant national events may include a major sporting event or political conventions, which may impact what facilities and sectors are approached for activities.

Agency Comments

The Department of Homeland Security reviewed a draft of this briefing and said that it concurred with the overall findings and conclusions of the briefing. We also received technical comments from DHS officials and incorporated them as appropriate.

GAO Contact and Staff Acknowledgements

- GAO Contact
 - Stephen L. Caldwell, (202) 512-8777 or CaldwellS@gao.gov
- Staff Acknowledgments
 - In addition to the contact named above, John F. Mortin, Assistant Director, and Anthony J. DeFrank, Analyst-in-Charge, managed this assignment with assistance from Andrew M. Curry, Luis E. Rodriguez, and Kendal B. Robinson. Michele C. Fejfar provided assistance with design and methodology. Thomas F. Lombardi provided legal support and Labony Chakraborty provided assistance in slide preparation.

RELATED GAO PRODUCTS

Critical Infrastructure Protection and Resiliency

- *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened.* GAO-10-772. Washington, D.C.: September 23, 2010.
- *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience.* GAO-10-296. Washington, D.C.: March 5, 2010.
- *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report.* GAO-09-654R. Washington, D.C.: June 26, 2009.
- *Information Technology: Federal Laws, Regulations, and Mandatory Standards to Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors.* GAO-08-1075R. Washington, D.C.: September 16, 2008.
- *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security.* GAO-08-904T. Washington, D.C.: Jun 25, 2008.
- *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.

RELATED GAO PRODUCTS (continued)

Critical Infrastructure Protection and Resiliency

- *Critical Infrastructure: Challenges Remain in Protecting Key Sectors.* GAO-07-626T. Washington, D.C.: March 20, 2007.
 - *Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks.* GAO-07-375. Washington, D.C.: January 24, 2007.
 - *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.* GAO-07-39. Washington, D.C.: October 16, 2006.
 - *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information.* GAO-06-383. Washington, D.C.: Apr 17, 2006.
 - *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* GAO-06-91. Washington, D.C.: Dec 15, 2005.
 - *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges.* GAO-05-327. Washington, D.C.: March 28, 2005.
 - *Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security.* GAO-05-33. Washington, D.C.: January 14, 2005.
-

GAO on the Web

Web site: <http://www.gao.gov/>

Contact

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

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

Copyright

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.

Comments from the Department of Homeland Security

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



**Homeland
Security**

May 5, 2011

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

Dear Mr. Caldwell:

Re: Draft Report GAO-11-537R, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*

The Department of Homeland Security (DHS), specifically the National Protection and Programs Directorate and U.S. Coast Guard, appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) subject draft report. The draft report contains no recommendations; however, we appreciate the recognition that the Department:

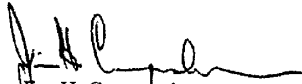
- coordinates with Critical Infrastructure and Key Resources (CIKR) stakeholders, including other federal regulatory authorities, through information-sharing mechanisms;
- is taking action to address overlapping security activities by clarifying roles and responsibilities for CIKR security activities with agencies with regulatory oversight through various coordination mechanisms; and
- works to address gaps in infrastructure security by developing and distributing tools that promote common security activities, and takes other steps including providing information on resources available to security partners and conducting vulnerability assessments at public and privately owned facilities that voluntarily participate.

As part of the continuous improvement feedback loop in the National Infrastructure Protection Plan's risk management framework, the annual assessment of progress feeds into the identification of opportunities for improvement and guides future risk management activities. The Department's continual work to address overlaps and gaps is an important part of our efforts to ensure that we enhance the protection and resilience of our Nation's critical infrastructure.

DHS concurs with the overall findings and conclusions of the draft report. Technical comments have been submitted under separate cover.

Thank you for the opportunity to comment on this draft report. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

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.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

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

Public Affairs

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