United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2012

CRITICAL INFRASTRUCTURE PROTECTION

An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure

GAO-13-11

October 2012

CRITICAL INFRASTRUCTURE PROTECTION

An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-11, a report to congressional requesters

Why GAO Did This Study

U.S. ports are part of an economic engine handling more than $700 billion in merchandise annually, and a disruption to port operations could have a widespread impact on the global economy. DHS has broad responsibility for protection and resilience of critical infrastructure. Within DHS, the Coast Guard is responsible for the maritime environment, and port safety and security, and IP works to enhance critical infrastructure resilience. Recognizing the importance of the continuity of operations in critical infrastructure sectors, DHS has taken initial steps to emphasize the concept of resilience. GAO was asked to review port resilience efforts. This report addresses the extent to which (1) DHS has provided a road map or plan for guiding resilience efforts, and (2) the Coast Guard and IP are working with port stakeholders and each other to enhance port resilience. To address these objectives, GAO analyzed key legislation and DHS documents and guidance. GAO conducted site visits to three ports, selected based on geography, industries, and potential threats; GAO also interviewed DHS officials and industry stakeholders. Information from site visits cannot be generalized to all ports, but provides insights.

What GAO Recommends

GAO recommends that DHS develop an implementation strategy for its resilience policy and that the Coast Guard and IP identify opportunities to collaborate to leverage existing tools and resources to assess port resilience. DHS concurred with GAO's recommendations.

View GAO-13-11. For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) is developing a resilience policy, but an implementation strategy is a key next step that could help strengthen DHS resilience efforts. DHS defines resilience as the ability to resist, absorb, recover from, or adapt to adversity, and some high-level documents currently promote resilience as a key national goal. Specifically, two key White House documents emphasize resilience on a national level—the 2011 Presidential Policy Directive 8 and the 2012 *National Strategy for Global Supply Chain Security.* Since 2009, DHS has emphasized the concept of resilience and is currently in the process of developing a resilience policy, the initial steps of which have included creating two internal entities—the Resilience Integration Team and the Office of Resilience Policy (ORP). According to ORP officials, they saw a need to establish a policy that provides component agencies with a single, consistent, departmentwide understanding of resilience that clarifies and consolidates resilience concepts from high-level guiding documents, and helps components understand how their activities address DHS's proposed resilience objectives. ORP officials hope to have an approved policy in place later this year. However, DHS officials stated that currently there are no plans to develop an implementation strategy for this policy. An implementation strategy that defines goals, objectives, and activities; identifies resource needs; and lays out milestones is a key step that could help ensure that DHS components adopt the policy consistently and in a timely manner. For example, an implementation strategy with goals and objectives could provide ORP with a more complete picture of how DHS components are implementing this policy.

The Coast Guard and the Office of Infrastructure Protection (IP) work with stakeholders to address some aspects of critical infrastructure resilience, but they could take additional collaborative actions to promote portwide resilience. The Coast Guard is port focused and works with owners and operators of assets, such as vessels and port facilities, to assess and enhance various aspects of critical infrastructure resilience in ports—such as security protection, port recovery, and risk analysis efforts. In contrast, IP, through its Regional Resiliency Assessment Program (RRAP), conducts assessments with a broader regional focus, but is not port specific. An RRAP assessment is conducted to assess vulnerability to help improve resilience and allow for an analysis of infrastructure "clusters" and systems in various regions—for example, a regional transportation and energy corridor. The Coast Guard and IP have collaborated on some RRAP assessments, but there may be opportunities for further collaboration to conduct port-focused resilience assessments. For example, IP and the Coast Guard could collaborate to leverage existing expertise and tools—such as the RRAP approach—to develop assessments of the overall resilience of specific port areas. Having relevant agencies collaborate and leverage one another's resources to conduct joint portwide resilience assessments could further all stakeholders' understanding of interdependencies with other port partners, and help determine where to focus scarce resources to enhance resilience for port areas.

Contents

Abbreviations

AMSC	Area Maritime Security Committee
DHS	Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection
FEMA	Federal Emergency Management Agency
IP	Office of Infrastructure Protection
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act of 2002
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
ORP	Office of Resilience Policy
PPD-8	Presidential Policy Directive 8
PRMP	Portwide Risk Mitigation Plan
PSA	Protective Security Advisor
PSGP	Port Security Grant Program
QHSR	Quadrennial Homeland Security Review
RIT	Resilience Integration Team
RRAP	Regional Resiliency Assessment Program
SAFE Port Act	Security and Accountability for Every Port Act of 2006
SSA	Sector-Specific Agency

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 25, 2012

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable John L. Mica
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Frank A. LoBiondo
Chairman
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
House of Representatives

U.S. ports, waterways, and vessels are part of an economic engine handling more than $700 billion in merchandise annually, according to the Department of Homeland Security (DHS), and a major disruption to this system could have a widespread impact on global shipping, international trade, and the global economy. For example, a 2006 report by the Congressional Budget Office estimated that a 1-week halt to all container traffic through the Ports of Los Angeles and Long Beach would result in a loss of gross domestic product of $65 million to $150 million per day.[1] This type of potential economic impact caused by a disruption in port operations underscores the importance of ensuring that ports remain operational to the maximum extent possible. Recognizing the importance of the continuity of operations in the maritime critical infrastructure subsector, among other sectors, DHS has begun to take steps to emphasize the concept of resilience—defined by DHS as the ability to

[1]Congressional Budget Office, *The Economic Costs of Disruptions in Container Shipments* (Washington, D.C.: Mar. 29, 2006).

resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.[2]

DHS has broad responsibility for protection and resilience of critical infrastructure in the United States. Within DHS, the U.S. Coast Guard is responsible for the maritime environment and the safety and security of ports, including recovery after an incident. The Office of Infrastructure Protection (IP) in the National Protection and Programs Directorate employs a number of activities designed to enhance critical infrastructure resilience across a number of sectors. At the department level, DHS focuses on an all-hazards approach to infrastructure protection and risk management, as enhancing resilience is one way to increase protection and reduce risks. Accordingly, each of the four elements of DHS's resilience definition broadly corresponds to some resilience-enhancing measure. For example, resilience involves preparation before, mitigation during, response immediately following, and recovery after an adverse event. Another key aspect of critical infrastructure resilience relative to ports involves understanding the interdependencies that exist between assets and critical infrastructure sectors (e.g., energy and water) necessary for operation of the port system as a whole. Generally, these interdependencies span wide geographic areas that can encompass the entire port and also extend beyond the port area.

We previously reported on DHS's evolving efforts to emphasize the importance of and promote resilience among critical infrastructure stakeholders through the *National Infrastructure Protection Plan* (NIPP)[3] and programs and assessments used to work with asset owners and

[2]DHS has identified 18 critical infrastructure sectors, which include Food and Agriculture; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons, Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; and Water. The Maritime subsector falls under the Transportation Systems sector.

[3]DHS, *National Infrastructure Protection Plan*, *Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). The NIPP provides DHS's overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort.

operators.[4] We found, among other things, that efforts to incorporate resilience into these programs and assessments were evolving. Additionally, we found that DHS was developing or updating programs to assess vulnerability and risk at critical infrastructure facilities and within groups of related infrastructure, regions, and systems to place greater emphasis on resilience. However, we also found that program management could be strengthened. We recommended that IP develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resilience gaps, and also update guidance for its Protective Security Advisors (PSA), who serve as liaisons between DHS and security stakeholders—to include asset owners and operators—in local communities. DHS concurred with these recommendations and has implemented one of them by providing resilience training to all PSAs. We also recommended that DHS assign responsibility to one or more components to determine the feasibility of overcoming barriers and developing an approach for disseminating information on resilience practices to critical infrastructure owners and operators. DHS responded that it is internally considering how it might implement this recommendation.

Given DHS's increased focus on resilience since 2009, you asked us to examine the issue of recovery and resilience in the port environment. Our first report, issued in April 2012, focused on Coast Guard efforts to address recovery and salvage planning.[5] This report addresses the extent to which

- DHS has provided a road map or plan for guiding component resilience efforts, and
- the Coast Guard and IP are working with port area stakeholders and each other to enhance resilience efforts at individual ports.

[4]See GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience,* GAO-10-296 (Washington, D.C.: Mar. 5, 2010), and *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened,* GAO-10-772 (Washington, D.C.: Sept. 23, 2010).

[5]GAO, *Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response*, GAO-12-494R (Washington, D.C.: Apr. 6, 2012).

To address these objectives, we reviewed key planning documents governing DHS efforts to assess critical infrastructure resilience (e.g., the NIPP and the *Quadrennial Homeland Security Review* [QHSR]), a draft policy on resilience, and an IP resilience assessment containing port-related information.[6] We also reviewed legislation and guidance governing Coast Guard security, recovery, and risk assessment efforts, as well as proposed guidelines for a Coast Guard–Canadian initiative being developed to enhance maritime port resilience. We have also incorporated information from our recent work on various Coast Guard and IP efforts to enhance security or resilience of critical infrastructure assets; these reports contain more detailed information on the methodologies used in their preparation.[7] We compared the existing draft policy and other documents on DHS resilience efforts (supplemented by information gathered through interviews, discussed below) with criteria for effective program management; specifically, our prior work on the characteristics of effective strategies[8] and our *Standards for Internal Control in the Federal Government*.[9] We also reviewed third-party work on federal efforts to enhance critical infrastructure resilience from the

[6]DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, (Washington, D.C.: February 2010). The QHSR report outlines a strategic framework for homeland security to guide the activities of homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations. It offers a vision for a secure homeland, specifies key mission priorities, and outlines goals for each of those mission areas.

[7]GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011), and *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments,* GAO-12-378 (Washington, D.C.: May 31, 2012).

[8]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

National Infrastructure Advisory Council (NIAC) and the State, Local, Tribal, and Territorial Government Coordinating Council.[10]

We supplemented our document reviews with interviews of officials at relevant organizational units at DHS headquarters, including the Office of Policy, IP, and the Coast Guard. At the field level, we conducted site visits to meet with Coast Guard and IP officials from a sample of three Group I (highest-risk) ports—New Orleans, Louisiana; Puget Sound, Washington; and the Delaware Bay region to discuss various efforts to work with port area stakeholders in enhancing port resilience.[11] The sample was selected to represent a mix of geographic diversity; industries (e.g., cruise ship, petroleum, and container), potential threats (earthquake, hurricane, or terrorism), and varied Coast Guard command units. During these port visits, we also interviewed officials from approximately four to five different industry stakeholders (owners/operators of assets such as container terminals or refineries, marine exchanges, port representatives, etc.) to gather their views on Coast Guard or IP efforts to address port resilience through assessments or stakeholder groups. In addition, we interviewed Coast Guard and IP officials at the four remaining Group I port areas. While the information gathered from Group I port interviews cannot be generalized to all maritime ports, it provided important perspective to our analysis.

[10]NIAC provides the President, through the Secretary of DHS, with advice on the security of critical infrastructure and also advises the lead federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. NIAC consists of state, local, and private sector (including industry and academia) representatives with expertise in critical infrastructure security and resilience. The State, Local, Tribal, and Territorial Government Coordinating Council is a forum for state, local, tribal, and territorial homeland security representatives to provide their expertise and experience to DHS in better protecting the nation's critical infrastructure.

[11]To promote a regional approach to port security, DHS aggregates individual ports into "port areas" for grant funding purposes. DHS determines the level of risk faced by U.S. port areas and then assigns those port areas to one of three groups (Groups I, II, and III) based on that risk, with Group I representing the highest risk. There are seven Group I port areas in the United States—Delaware Bay (which includes Philadelphia, Pennsylvania; Trenton, New Jersey; Wilmington, Delaware; and other ports in the region); Houston-Galveston, Texas; Los Angeles-Long Beach, California; New Orleans, Louisiana (which includes Baton Rouge and other ports); New York, New York, and New Jersey; Puget Sound (which includes Seattle, Olympia, Tacoma, and other ports in Washington); and San Francisco Bay, California (which also includes Oakland and other ports in California). We interviewed officials from the seven Coast Guard sectors that correspond with these Group I port areas.

We conducted this performance audit from April 2012 through October 2012, 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 and conclusions based on our audit objectives.

Background

Federal Legislation, Roles, and Responsibilities for Critical Infrastructure Protection and Port Security

The Homeland Security Act of 2002 provides the basis for DHS responsibilities in the protection of the nation's critical infrastructure.[12] The act assigns DHS responsibility for developing a comprehensive national plan for securing critical infrastructure and for recommending the measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities.[13] Other legislation enacted over the last decade has produced major changes in the nation's approach to maritime security. Much of the federal framework for port security is contained in the Maritime Transportation Security Act of 2002 (MTSA).[14] The MTSA establishes requirements for various layers of maritime security, including requiring a national security plan, area security plans, and facility and vessel security plans.[15] DHS has placed some responsibility for this and other MTSA requirements with the Coast Guard. In October 2006, the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) further refined the nation's port security framework, creating and codifying certain port security programs and initiatives.[16] For example, the SAFE Port Act required the development of protocols for

[12]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.

[13]6 U.S.C. § 121.

[14]Pub L. No. 107-295, 116 Stat. 2064 (2002).

[15]46 U.S.C. § 70103.

[16]Pub. L. No. 109-347, 120 Stat. 1884 (2006).

resumption of trade following a transportation security incident,[17] as well as Salvage Response Plans.[18]

DHS emphasizes the importance of resilience through key documents like the NIPP, QHSR, and directives. As the lead federal agency for the Marine Transportation System, the Coast Guard is responsible for facilitating the recovery of the system following a significant transportation disruption and working with maritime stakeholders in the resumption of trade.[19] The Coast Guard is also the Sector-Specific Agency (SSA) for the Maritime subsector of the Transportation sector and coordinates the preparedness activities among the sector's partners to prevent, protect against, respond to, and recover from all hazards that could have a debilitating effect on homeland security, public health and safety, or economic well-being.[20]

[17]6 U.S.C. § 942.

[18]46 U.S.C. § 70103(b)(2)(G). These Salvage Response Plans are to identify salvage equipment capable of restoring operational trade capacity, and to ensure that waterways are cleared and the flow of commerce through U.S. ports is reestablished as efficiently and quickly as possible after a maritime transportation security incident.

[19]While our review focused on DHS's efforts to establish resilience policy and enhance portwide resilience, other federal agencies have missions that relate, in part, to port operations. For example, the Department of Transportation Maritime Administration seeks to improve the U.S. maritime transportation system—including infrastructure, industry, and labor—to help meet the economic and security needs of the nation, among other things. This could include assisting state and local authorities with managing port infrastructure projects. In addition, the U.S. Army Corps of Engineers holds the primary federal responsibility for maintaining the navigability of federal channels—such as ensuring removal of an obstruction creating a hazard to navigation—in domestic ports and waterways. We currently have work ongoing reviewing these two agencies' efforts to maintain or improve the maritime transportation system, with a report to be issued later this year.

[20]The SSA is the federal department or agency identified in Homeland Security Presidential Directive-7 as responsible for critical infrastructure protection activities in specified critical infrastructure sectors. SSAs develop augmenting plans—called Sector-Specific Plans—that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each critical infrastructure sector. Sector-Specific Plans are developed by the SSAs in close collaboration with other sector partners. Homeland Security Presidential Directive-7 also directs SSAs to provide an annual report—the Sector Annual Report—to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate critical infrastructure protection and resilience in their respective sectors.

IP is responsible for working with public and private sector critical infrastructure partners and leads the coordinated national effort to mitigate risk to the nation's critical infrastructure. IP also has the overall responsibility for coordinating implementation of the NIPP across 18 critical infrastructure sectors; overseeing the development of 18 Sector-Specific Plans; providing training and planning guidance to SSAs and owners and operators on protective measures to assist in enhancing the security of critical infrastructure within their control; and helping state, local, tribal, territorial, and private sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to their assets.

IP's Protective Security Coordination Division provides programs and initiatives to enhance critical infrastructure protection and resilience and reduce risk associated with all-hazards incidents. To carry out these responsibilities, IP has deployed PSAs in 50 states and Puerto Rico, with deployment locations based on population density and major concentrations of critical infrastructure. One PSA duty is to coordinate and conduct voluntary assessment services to assist critical infrastructure owners and operators in reviewing and strengthening their security posture. Specifically, PSAs coordinate and carry out various IP protective programs such as the Enhanced Critical Infrastructure Protection (ECIP) initiative, which is a voluntary program focused on forming or maintaining partnerships between DHS and critical infrastructure owners and operators of high-priority assets and systems, as well as other assets of significant value.[21] The PSAs also coordinate and participate in Site Assistance Visit vulnerability assessments to identify security gaps and provide options for consideration to mitigate these identified gaps.[22]

[21]If an asset owner or operator agrees to participate in an ECIP visit, PSAs are to meet with the owner or operator to assess overall site security, identify gaps, provide education on security, and promote communication and information sharing among asset owners and operators, DHS, and state governments. One of the components of the ECIP Initiative is the security survey, which uses the Infrastructure Survey Tool—an electronic data collection platform that a PSA uses to gather information on the asset's current security posture and overall security awareness.

[22]IP teams conduct the assessments in coordination with PSAs; SSAs; state and local government organizations (including law enforcement and emergency management officials); asset owners and operators; and the National Guard, which is engaged as part of a joint initiative between DHS and the National Guard Bureau.

These assessments are on-site, asset-specific, nonregulatory assessments conducted at the request of asset owners and operators.[23]

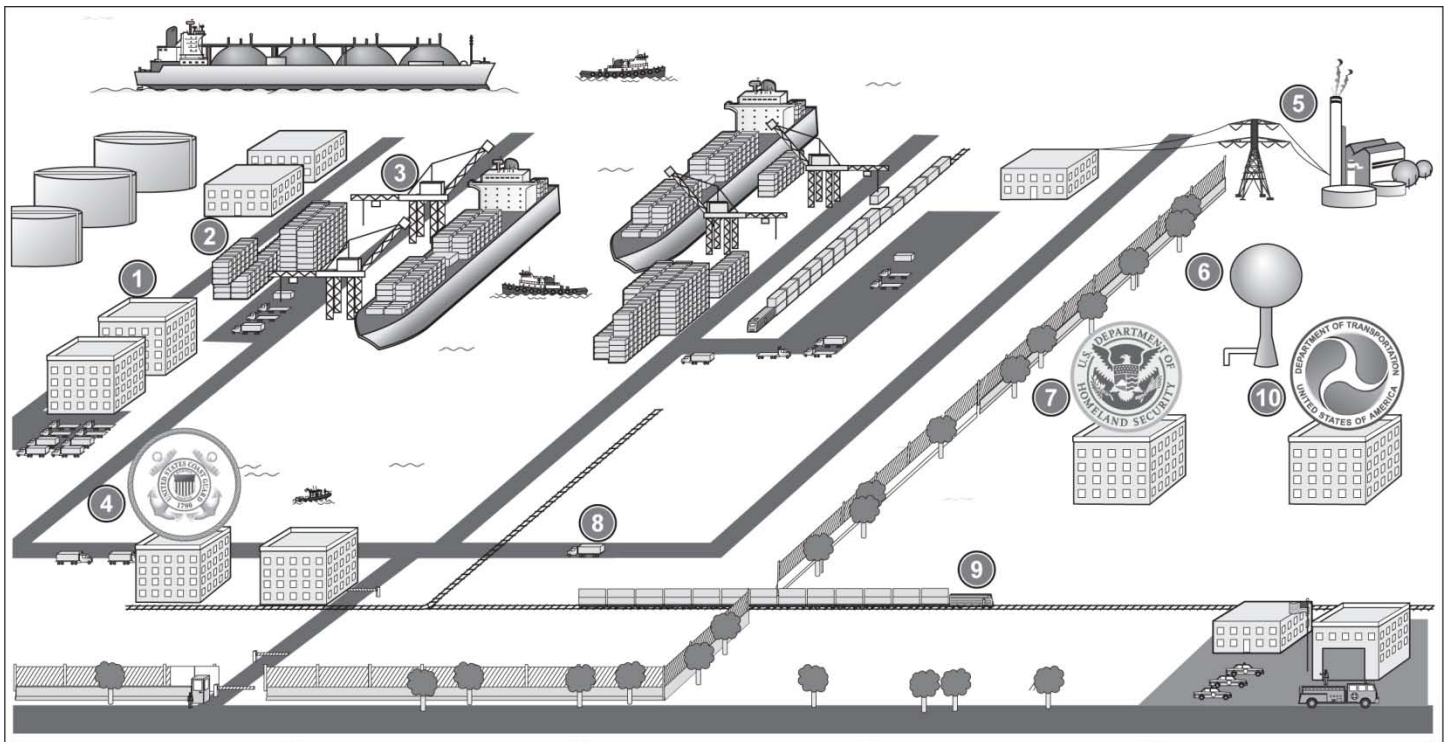
Port Area Operations Cross Several Critical Infrastructure Sectors

Port operations involve a complicated system of systems, which operates across multiple sectors. The port area consists of many assets that are interdependent with other sectors, such as power and water, to continue normal operations. For example, container terminals have large energy needs to operate the cranes that load and unload cargo. In most cases, backup generators cannot produce enough power to keep these cranes operational, so reliable energy production and transportation are vital to maintaining normal port operations. Similarly, refinery, chemical plant, cruise line, ferry, and other port operations also have high energy and water needs. In addition, many port operations rely heavily upon trucking and rail transportation to move personnel and cargo in and out of the port area. Furthermore, the availability of a functional labor force and information technology support—which may be located within or outside of a port area—is important for port stakeholders' operations.

Similarly, many businesses and communities rely on the port for their normal operations. Energy, food, and product shipments are vital to port operations, port stakeholders, and the broader community. Interruptions in the supply chain often have secondary and tertiary impacts that may not be immediately obvious to businesses and communities. Figure 1 illustrates some of the key stakeholders within a port and the importance of their interactions. Understanding the interdependencies among various port area stakeholders and other critical partners outside the port area is necessary to ensure and enhance a port's resilience.

[23]In May 2012, we reviewed IP's efforts to conduct these security surveys and vulnerability assessments of critical infrastructure and noted challenges in the program, such as inconsistencies in data collection efforts, late delivery of survey and assessment results to asset owners and operators, and a need to capture additional information when following up with stakeholders. We recommended that, among other things, DHS develop plans for its efforts to improve the collection and organization of data and the timeliness of survey and assessment results, and gather and act upon additional information from asset owners and operators about why improvements were or were not made. DHS concurred with the recommendations. See GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments,* GAO-12-378 (Washington, D.C.: May 31, 2012).

Figure 1: Key Partners Involved in Port Critical Infrastructure Operations and Oversight



1 Shipping companies

Facilitate bringing goods to and from the port.

2 Container terminals

Areas used to load and unload cargo from ships.

3 Crane operators

Operators use cranes to transfer containers and other types of cargo between ships and trucks or trains.

4 Coast Guard

Provides federal oversight of portwide safety and security.

5 Power

Port area facilities and assets depend on power to operate.

Power providers can be located outside the port area.

6 Water

Port area facilities and assets depend on water to operate.

Water providers can be located outside the port area.

7 DHS Office of Infrastructure Protection

National coordinator for the protection and resilience of critical infrastructure.

8 Trucking companies

Transport goods within the port and from the port to inland locations.

9 Rail carriers

Transport goods from the port to inland locations.

10 Department of Transportation

Enforces federal safety regulations or standards for the trucking and rail industries, among other things.

Source: GAO.

DHS Is Developing a Resilience Policy, but an Implementation Strategy Could Help Ensure Consistency and Accountability

High-Level Documents Promote Resilience, and DHS Has Begun to Develop a Resilience Policy

National high-level documents currently promote resilience as a key national goal. Specifically, two key White House documents emphasize resilience on a national level—Presidential Policy Directive 8 (PPD-8) and the *National Strategy for Global Supply Chain Security*.[24]

- PPD-8 defines resilience as the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.
- The *National Strategy for Global Supply Chain Security* endorses building a layered defense, addressing threats early, and fostering a resilient system that can absorb and recover rapidly from unanticipated disruptions.

Key federal entities, including DHS, are currently working to develop frameworks or other strategies for implementing the goals and objectives of these documents, which should provide greater insights into how they plan to strengthen national resilience.

Since 2009, DHS has also emphasized the concept of resilience through two high-level documents—the NIPP and QHSR.

[24]See the White House, *Presidential Policy Directive/PPD-8, Subject: National Preparedness* (Washington, D.C.: Mar. 30, 2011). PPD-8 calls for the development of a national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the nation to achieve this goal. See also the White House, *National Strategy for Global Supply Chain Security* (Washington, D.C.: Jan. 23, 2012). This strategy articulates the federal government's policy for strengthening the global supply chain, focused on the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructure by which goods are moved as well as supporting communications infrastructure and systems.

- The NIPP identifies resilience as a national objective for critical infrastructure protection and defines resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

- The QHSR identifies ensuring resilience to disaster as one of the nation's five homeland security missions.[25] The QHSR also defines resilience as fostering individual, community, and system robustness, adaptability, and capacity for rapid recovery.

According to DHS, resilience is one of the foundational elements for a comprehensive approach to homeland security; thus, its missions and programs designed to enhance national resilience span the department. Accordingly, DHS is currently developing a policy to bring a cohesive understanding of resilience to its components and establish resilience objectives. DHS took steps to foster departmentwide resilience initiatives by creating two internal entities—the Resilience Integration Team (RIT) and the Office of Resilience Policy (ORP). In April 2010, DHS formed RIT to develop new initiatives that support the overarching resilience mission set forth in the QHSR. To date, RIT has been the key DHS-wide working group charged with developing and disseminating resilience concepts.[26] According to agency officials, RIT brings together subject matter experts from all components whose missions affect resilience in some manner for

[25]The five homeland security missions are (1) preventing terrorism and enhancing security, (2) securing and managing our borders, (3) enforcing and administering our immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters.

[26]Aside from working on a resilience policy, RIT has two key efforts under way. First, in early 2011, RIT established the Resilient STAR designation—a voluntary certification program that aims to make homes and buildings more secure and resilient to all hazards. The program is in the early stages of development and has only been piloted in the private residential sector, but the team plans to expand the designation to other sectors, including the maritime environment. However, according to agency officials, resource constraints have prevented them from expanding more rapidly. RIT is also working with Sandia National Laboratories and ORP to indentify resilience criteria that could be used for the Resilient STAR program. This effort involves evaluating existing industry standards pertinent to a sector and making a determination of their usefulness for the Resilient STAR designation. Second, RIT is also working to update the definition of resilience in the DHS Risk Lexicon. According to agency officials, DHS will soon add an alternative definition for resilience that will expand on the definition already in use throughout DHS.

monthly meetings. DHS formed ORP in March 2012 to coordinate and promulgate resilience strategies throughout the department.[27]

In 2010, RIT officials surveyed components about how their activities addressed resilience in an attempt to gauge components' understanding of resilience, as discussed in the QHSR. According to RIT officials, component responses showed that component resilience actions were very diverse and represented stovepiped efforts that were still "works in progress." ORP officials told us that these differing approaches to implementing and identifying resilience efforts were part of the reason they saw a need for one DHS resilience policy. Specifically, ORP saw a need to establish a policy that provides component agencies with a single, consistent, departmentwide understanding of resilience; clarifies and consolidates the concepts from the four high-level guiding documents discussed above; and helps components understand how their activities address DHS's proposed resilience objectives. The policy is currently in draft status, and ORP officials hope to have an approved policy in place later this year.

Developing a Strategy Could Help Guide Components' Efforts in Implementing DHS's Resilience Policy

Although DHS is developing a policy to establish a departmentwide resilience framework, DHS officials stated that they currently have no plans to develop an implementation strategy for DHS's resilience policy. An implementation strategy that defines goals, objectives, and activities could help ensure that the policy is adopted consistently and in a timely manner by components, and that all components share common priorities and objectives. Additionally, an implementation strategy with specific milestones could help hold ORP and DHS components accountable for taking actions to address resilience objectives identified in the new policy in a timely manner. ORP officials acknowledged that an implementation strategy could be beneficial because it could provide concrete steps for employing DHS's new resilience policy and harmonizing component efforts.

[27]According to ORP officials, ORP is also working to incorporate resilience incentives and requirements into DHS's grant programs.

In previous work, we identified key characteristics that should be included in a strategy, as discussed below.[28]

- *Goals, subordinate objectives, activities, and performance measures* set clear desired results and priorities, specific milestones, and outcome-related performance measures while giving implementing parties flexibility to pursue and achieve those results within a reasonable time frame.

- *Organizational roles, responsibilities, and mechanisms for coordinating their efforts* identify the relevant departments, components, or offices and, where appropriate, the different sectors, such as state, local, private, or international sectors. The strategy would also clarify implementing organizations' relationships in terms of leading, supporting, and partnering.

- *Resources, investments, and risk management* identify, among other things, the sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted.

As DHS implements its resilience policy, an implementation strategy with these characteristics could provide ORP with a clear and more complete picture of how DHS components are implementing this policy, as well as how the various programs and activities are helping to enhance critical infrastructure resilience in their areas of responsibility. For example, establishing desired results and priorities, such as departmentwide resilience objectives, could help components better understand and communicate how their actions and strategies fulfill those policy objectives. It could also help ORP maintain awareness of various component actions and how these actions align with the policy while also helping components identify which actions are most critical to addressing these objectives. Additionally, milestones could help to ensure that ORP is receiving timely input from components regarding their actions to

[28]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004). This report contained other criteria that could apply to the development of national strategies. For the purposes of this report, we selected those criteria that we believe are the most applicable to current DHS efforts to develop an implementation strategy for its resilience policy at this point in time.

address resilience objectives, and help ORP and components determine whether adjustments to the policy are needed.

Furthermore, as part of the strategy, developing performance measures, such as the number of components that have reported back on resilience efforts, would help provide ORP with more complete information for gauging the level of component acceptance of the policy and understanding of how components' actions address resilience objectives. Moreover, identifying relevant government entities and implementing organizations could provide components with clear expectations for collaborating with other partners inside and outside of DHS, and reporting this collaboration back to ORP. This step could also clearly define departmental components responsible for promoting resilience by identifying critical stakeholders and subject matter experts within and outside of DHS. Moreover, clarifying relationships among components, other government entities, and private partners could foster a greater understanding of their dependence on one another and provide valuable perspective for ORP. Finally, identifying the types of resources and investments needed, and where they should be targeted, could help provide guidance to the implementing components to manage resources and lead them to consider where resources should be invested now and in the future based on balancing risk reductions and costs. ORP officials stated that they have focused initial efforts on developing the resilience policy, and had not given consideration to developing an implementation strategy for this policy. Going forward, we believe that focusing efforts on developing an implementation strategy that includes the elements we identified could benefit DHS components' efforts to enhance resilience.

The Coast Guard and IP Have Addressed Some Aspects of Critical Infrastructure Resilience, but Could Better Coordinate to Promote Portwide Resilience

The Coast Guard Works with Stakeholders to Address Aspects of Resilience

The Coast Guard works with asset owners and operators to assess and enhance various aspects of port critical infrastructure resilience—such as security protection, port recovery, and risk analysis efforts, as described in table 1.

Table 1: Coast Guard–Related Efforts That Address Elements of Resilience with Port Stakeholders

Initiative	Description
Area Maritime Security Committee (AMSC)	AMSCs are required to provide advice to and assist the Captain of the Port in the development, review, and update of the Area Maritime Security Plan for the committees' areas of responsibility; assist with the identification of risks; and determine mitigation strategies, among other things.[a] AMSCs are also required to meet at least annually or when requested by a majority of members, providing port stakeholders with a forum for cooperative engagement with the Coast Guard for overall port security. AMSCs are to include a number of different port stakeholders and governmental entities charged with varying responsibilities within the marine transportation system. A combination of federal, state, local, territorial, and tribal, as well as private sector, entities (e.g., vessel agents, terminal operators, and marine exchanges) may be represented on each AMSC.
Area Maritime Security Plans[b]	Prepared by the Coast Guard with input from applicable governmental and private entities, including the AMSCs, these plans serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response, as well as facilitation of marine transportation system recovery and salvage elements.[c]
Facility Security Plan Reviews	Federal law requires that certain facilities establish these plans, and the Coast Guard is responsible for reviewing and approving the plans, ensuring their implementation, verifying continued adherence to the plans, and periodically reapproving the plans.[d]
Port security exercises	The Coast Guard is required to conduct exercises to enhance port security under the SAFE Port Act.[e] The Coast Guard sponsors these exercises to, among other things, assist port stakeholders in identifying and addressing resilience-related issues, such as recovery and continuity of operations. Coast Guard and industry officials stated that these exercises can be particularly helpful in getting stakeholders with a nexus to maritime activity but perhaps not located directly on the waterfront (e.g., trucking and rail companies) involved in discussing port resilience issues.
Port Security Grant Program (PSGP)	The PSGP was established to allocate funds based on risk to implement Area Maritime Security Plans and facility security plans.[f] While the Federal Emergency Management Agency (FEMA) is the program manager and awards port area grants, the Coast Guard has a significant role in determining how funds will be allocated within a port area by ensuring that projects comply with Area Maritime Security Plans and facility security plans. The PSGP funds maritime security risk mitigation projects that support port resilience and recovery efforts, and some PSGP grants have helped to fund projects that strengthen resilience throughout a port region (e.g., a private entity's installation of a waterside camera system that can be monitored by emergency responders and other port partners). Through the PSGP, FEMA has required the highest-risk ports to prepare Portwide Risk Mitigation Plans (PRMP), to help identify and execute actions to mitigate maritime critical infrastructure risks. Specifically, the PRMP requirement was part of a broader effort to shift grant funding from supporting asset-specific projects that benefit one facility to supporting more regional, portwide projects that would benefit an entire port area.
United States-Canada Maritime Commerce Resilience	In response to a high-level plan by the United States and Canada to enhance border security and trade efforts, Coast Guard and Canadian transportation officials are working together to develop guidelines to enhance communication and information sharing to help facilitate maritime trade recovery between the two nations after an emergency or disaster in ports that are close to one another.[g]
Maritime Security Risk Analysis Model (MSRAM)	A Coast Guard–developed risk-based decision support tool designed to help it assess and manage maritime security risks for key maritime infrastructure assets. MSRAM touches on some aspects of resilience, such as security, target hardness, and secondary economic impacts (including target redundancy), though it does not assess port systemwide effects of disruptions, nor was it intended to do this.

Source: GAO analysis of DHS information.

[a]33 C.F.R. §§ 103.300-.310. The AMSC is established, convened, and directed by the Captain of the Port, designated by 33 C.F.R. § 103.200 to serve as Federal Maritime Security Coordinator. The Captain of the Port is the Coast Guard officer designated by the Coast Guard Commandant to enforce, within his or her respective area, port safety, security, and maritime environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

[b]Area Maritime Security Plans are developed for each of the 43 individual Captain of the Port zones—specific port areas geographically defined in 33 C.F.R. part 3. These port zones generally correspond to the 35 Coast Guard sectors. However, separate Area Maritime Security Plans have also been developed for six Marine Safety Units—which represent distinct areas (zones) within those sectors—as well as the Gulf of Mexico and the Commonwealth of the Northern Mariana Islands.

[c]In April 2012, we reviewed the recovery and salvage elements of Area Maritime Security Plans for seven Group I port areas—those determined by DHS to be at the highest risk—and found that each addressed recovery and salvage response, as required by law, and incorporated the specific recovery and salvage response elements, as described in Coast Guard planning guidance. See GAO, *Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response*, GAO-12-494R (Washington, D.C.: Apr. 6, 2012).

[d]33 C.F.R. §§ 105.400-415. In general, facilities that receive vessels that carry large or hazardous cargo, vessels subject to international maritime security standards, selected barges, and passenger vessels certified to carry more than 150 passengers are subject to MTSA regulations. Owners or operators of such assets are required, among other things, to designate a facility security officer, ensure that a facility risk assessment is conducted, and ensure that a facility security plan is approved and implemented. 33 C.F.R. pt. 105.

[e]6 U.S.C. § 912.

[f]For more information on the PSGP, see GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, GAO-12-47 (Washington, D.C.: Nov. 17, 2011).

[g]The guidelines stem from *United States-Canada, Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, Action Plan, December 2011. The Action Plan established joint priorities within four areas of cooperation: addressing threats early; trade facilitation, economic growth, and jobs; cross-border law enforcement; and critical infrastructure and cyber security. In July 2012, Coast Guard and Transport Canada officials hosted the U.S.-Canada Maritime Commerce Resilience Workshop in Seattle, Washington, to discuss elements of these guidelines and generally work to enable collaboration at the regional level to expedite maritime commerce recovery following an emergency, disaster, or disruption. Representatives from both nations' governments, state and local entities, and industry groups attended this workshop, with an additional tabletop exercise planned for October 2012. The Coast Guard stated that following this exercise, it plans to expand these guidelines to other port areas with a nexus to Canada.

In general, officials from the seven Coast Guard sectors we interviewed and various industries at the three ports we visited cited the efforts depicted in table 1 as helpful in addressing or raising awareness of resilience-related issues (e.g., port security and recovery). Their views on the value of some of these key efforts are summarized below.

- *AMSCs*. Coast Guard officials we met with at each of the seven sectors stated that they maintain working relationships with port stakeholders via the AMSCs and other groups, which provide a forum for regular communication among port stakeholders on issues related to security and recovery—key elements of resilience. At the three ports we visited, industry stakeholders also cited the importance of the AMSCs in raising awareness of security or resilience issues. In

addition, our prior work has illustrated the importance of AMSCs in facilitating information sharing at the port level.[29] One example of Coast Guard efforts to promote resilience at the local level through the AMSC is occurring at Sector Delaware Bay. Coast Guard officials there reported working with members of the local maritime exchange to develop a guide to business continuity planning—an important element in enhancing resilience. According to sector officials, the guide was developed to assist smaller businesses in the port area that lacked the capability or funds to develop a business continuity plan in-house. Delaware Bay officials reported that they have shared this template with other Coast Guard sectors as well.

- *Port security exercises*. Officials from six of the seven sectors and industry officials at the three ports we visited cited the importance of addressing recovery and resilience planning issues through various training exercises, whether sponsored by the Coast Guard or other entities. For example, officials in one Coast Guard sector spoke about the importance of a training exercise focused on waterway recovery in getting intermodal stakeholders (such as container terminal operators) to think beyond impacts on their own facilities and consider the resilience of the port area as a whole (e.g., how the port would meet the needs of partners dependent on its shipping services).

- *PSGP*. Officials at five of the seven Coast Guard sectors—as well as industry stakeholders at the three ports we visited—cited the PSGP as an important means of addressing risk management and resilience issues in port areas. For example, one river pilots' association reported that it used PSGP funds to expand the use of a radar system for tracking vessels and provided access to the information to the Coast Guard, police, and other authorities. Thus, this system could both increase portwide awareness and aid in recovery efforts following an incident. In addition, officials at four Coast Guard sectors, as well as industry stakeholders, pointed to the PRMP as helpful in identifying security gaps and priorities to be addressed.

[29]GAO, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO-05-394 (Washington, D.C.: Apr. 15, 2005).

- *MSRAM*.[30] Coast Guard officials have stated that, as part of the evolution of MSRAM, it is taking preliminary steps to make MSRAM more helpful in assessing resilience. Specifically, the agency is considering ways to use MSRAM data and other tools to help mitigate the criticality or risk levels of key critical infrastructure while also improving its estimates of secondary economic impacts of an event. According to MSRAM program officials, these efforts are in very early stages.

IP Conducts Asset-Specific and Regional and Resilience Assessments

While not focused specifically on ports, IP assists critical infrastructure owners and operators of individual assets throughout the nation in understanding their own level of resilience through voluntary assessments and surveys. IP also conducts assessments of regional resilience in some areas of the country. As discussed earlier, IP employs voluntary assessments and security surveys aimed at helping these owners and operators identify and potentially address vulnerabilities, among other things. In addition, IP has two key efforts designed to help enhance resilience—its Resilience Index/Assessment Methodology and Regional Resiliency Assessment Program (RRAP), described below.

- *Resilience Index/Assessment Methodology*. IP has developed a Resilience Index for its vulnerability assessments and security surveys. This index is intended to provide the levels of resilience at critical infrastructure, guide prioritization of resources for improving critical infrastructure, and also provide information to owners/operators about their facility's standing relative to those of similar sector assets and how they may increase resilience.[31] IP is also in the process of developing a new Resilience Assessment

[30]In November 2011, we reviewed MSRAM and found that it generally aligns with DHS risk assessment criteria, but additional documentation on key aspects of the model could benefit users of the results. We recommended that the Coast Guard provide more thorough documentation on MSRAM's assumptions and other sources of uncertainty, make MSRAM available for peer review, implement additional MSRAM training, and report the results of its risk reduction performance measure in a manner consistent with risk analysis criteria. The Coast Guard agreed with these recommendations and is taking actions to implement them. See GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011).

[31]We have not assessed the methodology used to construct the Resilience Index, and thus cannot comment on the strengths or weaknesses of this approach to assess resilience.

Methodology to improve DHS's ability to assess asset-level resilience, inform regional resilience efforts, and measure progress in enhancing resilience.

- *RRAP*. These assessments are conducted to assess vulnerability to help improve resilience and allow for an analysis of infrastructure "clusters" and systems in various regions. This program, which uses vulnerability assessments and surveys, along with other tools, has included ports as a transportation hub element of a larger regional analysis, but has not yet been applied to focus solely on a port.[32] The RRAP evaluates critical infrastructure on a regional level to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resilience characteristics, and gaps. For example, an RRAP review could involve compiling information from reviews of critical infrastructure assets—such as electricity providers and transport companies—to form an overall assessment of a key transportation and energy corridor within a state. The RRAP assessments are conducted by DHS officials, including PSAs in collaboration with SSAs; other federal officials; state, local, territorial, and tribal officials; and the private sector, depending upon the sectors and assets selected as well as a resilience subject matter expert or experts.[33] The results of the RRAP are to be used to enhance the overall security posture of the assets, surrounding communities, and the geographic region covered by the project.

According to DHS officials, the results of specific asset-level assessments conducted as part of the RRAP are made available to asset owners and operators and other partners (as appropriate), but the final analysis and

[32]IP does not examine a port's security or other aspects that are the regulatory purview of other agencies.

[33]In conducting the RRAP, DHS does a comprehensive analysis of a region's critical infrastructure and protection and prevention capabilities and focuses on (1) integrating vulnerability and capability assessments and infrastructure protection planning efforts; (2) identifying options for consideration to improve prevention, protection, and resilience; (3) analyzing system recovery capabilities and providing options to secure operability during long-term recovery; and (4) assessing state and regional resilience, mutual aid, coordination, and interoperable communication capabilities. We have recently initiated work examining the criteria for the selection of RRAPs, how RRAPs identify vulnerabilities in security and resilience, the challenges DHS faces working with owners and operators to address the vulnerabilities identified by the RRAPs, and how DHS measures the effectiveness of RRAPs. We anticipate completion of this engagement in 2013.

report are delivered to the state where the RRAP occurred. Further, according to DHS, while it continues to perform surveys and assessments at individual assets, prioritizing efforts to focus on regional assessments allows DHS to continue to meet evolving threats and challenges. IP officials also informed us that through the RRAPs, the focus of its vulnerability assessment efforts has evolved over the years from a single-facility assessment to an approach that integrates the results of multiple single-facility assessments to inform a regional analysis of resilience and security through the study of dependencies and interdependencies between and among asset operators.

IP officials stated that the Coast Guard participates in RRAPs that include a maritime component. The officials have also informed us that the results of Coast Guard reports and assessments are included in the Resiliency Assessment (the RRAP final report) for RRAPs that include a maritime component, and the information is appropriately derived to alleviate any information-sharing concerns.[34] IP also reports that it has done some ECIPs/Site Assistance Visits at facilities associated with ports (e.g., refineries, storage facilities, and marine terminals). In addition, officials we spoke with from four Coast Guard sectors and PSAs representing five areas report maintaining relationships with one another through the AMSCs or other venues to facilitate information sharing.

DHS Components Have Opportunities to Collaborate and Leverage Existing Tools to Assess Port Resilience

While the Coast Guard and IP have collaborated on some regional resilience assessments, there may be opportunities for further collaboration and use of existing tools to conduct portwide resilience assessment efforts. For example, IP and the Coast Guard could leverage some of the expertise and tools discussed above—such as the RRAP approach—to develop assessments of the overall resilience of one or more specific port areas. Currently, many of the Coast Guard's formal security assessments (i.e., facility security plan reviews and MSRAM) are focused on asset-level security. For example, our prior work on MSRAM demonstrates that this tool assesses security risks to individual assets, not regions or systems of assets. In addition, the facility security plan reviews are not voluntary, but are conducted to fulfill regulatory requirements.

[34]For example, in one RRAP analysis, the Coast Guard provided the RRAP team with continuity-of-operations and security plans for the local port area that were used in an analysis of the port's overall contingency preparedness.

In contrast, IP's RRAP allows for a broader, more systemic analysis of resilience, and industry provides information to IP on a voluntary basis. IP officials stated that IP has not conducted any RRAPs focused exclusively on ports, and does not intend to, because of the Coast Guard's role as lead agency for ensuring port safety, recovery planning, and security, and because IP has limited resources for conducting additional RRAPs. However, IP has conducted RRAPs of regional corridors that have a nexus to a port or waterside critical infrastructure assets. For example, one recent RRAP review focused on a regional transportation and energy corridor and discussed the critical importance of a local port in providing fuel, medicine, and other "life-sustaining" goods throughout the state. The report found, among other things, that the port had no emergency power-generating capability; thus, a disruption to the power grid supporting port operations could seriously affect distribution of these life-sustaining goods to state residents. The report recommended that the port work to establish an agreement with another local entity to secure emergency power supplies. This work illustrates the potential vulnerabilities—and mitigation steps—that could be identified through a port-focused resilience review. In addition, NIAC supports further use of RRAPs, reporting that the RRAP is viewed in the field as a "model of collaboration" in understanding regional and community resilience and recommended that its use be expanded "as quickly as feasible." ORP officials have also stated that having Coast Guard and IP leverage resources and collaborate on systematic portwide resilience assessments could be beneficial.

In addition, during the course of our review, we learned of a state-led, ongoing effort to assess portwide resilience at one port area that could prove to be an example of beneficial collaboration that enhances the understanding of port resilience. The New Jersey Office of Homeland Security and Preparedness is leading an effort to develop a computer-based decision support tool that could model the impacts of various disruptions on all critical infrastructure owners and operators within the New York/New Jersey port area.[35] The project team—in collaboration with federal, state, local, and private stakeholders—is examining data from critical facilities and prior assessments to develop decision-making tools to model various scenarios. In addition, according to involved officials, the

[35]According to state officials, the project is supported by a FEMA grant, and also through combined efforts with a similar project supported by other DHS Homeland Security Grant Program funding.

model is designed to be expandable and transferrable to other ports. Project officials stated that cooperation by critical industry stakeholders has been a key factor in the project's development so far. These officials stated that they hope to develop three key tools: (1) a decision support tool that identifies port area vulnerabilities; (2) a port recovery and resumption-of-trade plan that helps to develop strategic issues to be addressed; and (3) a compendium of specific recommendations in the area of resilience, some aimed at specific facilities, some requiring portwide cooperation to address.

Various stakeholder groups have noted that in addition to the development of tools to enhance resilience, collaboration among partners is also key because of the expertise that each party can contribute to a better understanding of resilience. For example, NIAC and the State, Local, Tribal, and Territorial Government Coordinating Council have reported on a general lack of understanding by state and local community partners of the nature of interdependencies among infrastructure sectors and across communities. Both organizations recommended that IP take a lead role in developing tools and techniques that could help community partners at the state and local levels identify and assess infrastructure interdependencies.[36]

We have reported in the past on how collaborating agencies can better identify and address needs by leveraging one another's' resources to obtain additional benefits that would not be available if they were working separately.[37] *Standards for Internal Control in the Federal Government* also states that program management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving

[36]See NIAC, *Optimization of Resources for Mitigating Infrastructure Disruptions Study*, *Final Report and Recommendations by the Council*, Oct. 19, 2010; and State, Local, Tribal, and Territorial Government Coordinating Council, *Landscape of State and Local Government Critical Infrastructure Resilience Activities & Recommendations*, submitted to the DHS Office of Infrastructure Protection, May 2011. The latter document was prepared in response to an invitation from DHS to help IP formulate a cohesive approach to coordinating national infrastructure resilience efforts. In presenting this report, the council noted that its recommendations were broad and preliminary, and it planned to revise the paper based on further stakeholder input as needed.

[37]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

its goals.[38] Thus, a collaborative effort between the Coast Guard and IP to assess portwide resilience—leveraging tools and assessment approaches developed by either component, which could include MSRAM and the RRAP—could yield benefits. Specifically, the Coast Guard's assessments of port/maritime assets coupled with IP's assessments of other critical infrastructure with a port nexus could lead to a better understanding of the interdependencies critical to keeping a port operational. DHS officials have stated that any collaborative efforts to assess portwide resilience must take into account the difference between the Coast Guard's regulatory and IP's voluntary missions. For example, certain information gathered by IP from industry through voluntary assessments, surveys, or programs such as RRAP cannot be shared with the Coast Guard (or other federal entities) for regulatory purposes, though it can be shared for conducting other types of analyses, such as port security reviews.[39] We acknowledge this distinction and recognize that in structuring any such collaboration, DHS would have to protect such information. DHS's support for enhancing resilience is already evident in IP's voluntary assessments, as well as DHS's involvement in and endorsement of the New York/New Jersey port area project. Identifying opportunities to leverage tools and resources to collaboratively conduct portwide resilience assessments could enhance stakeholders' understanding of interdependencies with other port partners, and help to focus scarce resources to enhance resilience for the port area. This understanding is important to maintaining port operations, thus minimizing the potential adverse economic impact on the U.S. economy in the event of a disruption in port operations.

Conclusions

DHS has taken initial steps to emphasize the concept of resilience among its components by developing a resilience policy. This has been an important step and is appropriately intended to provide component agencies with a single, consistent, departmentwide understanding of resilience. Developing an implementation strategy for this new policy is the next key step that could help strengthen DHS's resilience efforts. For example, an implementation strategy that identifies goals and objectives could help DHS components to identify, among other things, the actions that are most critical to addressing DHS's policy objectives. Similarly, an

[38] GAO/AIMD-00-21.3.1.

[39] See 6 C.F.R. pt. 29.

implementation strategy that identifies responsible entities and their roles, as well as specific milestones and performance measures, could provide components with clear expectations for collaborating with other partners, and enhance DHS's awareness of components' understanding and implementation of the policy. This collective information, in turn, would allow DHS to better assess the progress being made by its components in addressing DHS resilience objectives.

At the port level, U.S. ports, waterways, and vessels are part of a major economic engine, and a significant disruption to this system could have a widespread impact on the U.S. economy, as well as global shipping, international trade, and the global economy. Coast Guard and IP actions have addressed some aspects of critical infrastructure resilience, but the Coast Guard and IP could take additional action to enhance their collaboration and use existing tools and resources to promote portwide resilience. For example, IP and the Coast Guard could leverage existing expertise and tools—such as IP's RRAP approach—to develop assessments of the overall resilience of one or more port areas. Having relevant agencies collaborate and leverage one another's resources to conduct joint portwide resilience assessments could further all stakeholders' understanding of interdependencies with other port partners, and better direct scarce resources to enhance port resilience.

Recommendations for Executive Action

To better ensure consistent implementation of and accountability for DHS's resilience policy, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for Policy to develop an implementation strategy for this new policy that identifies the following characteristics and others that may be deemed appropriate:

- steps needed to achieve results, by developing priorities, milestones, and performance measures;
- responsible entities, their roles compared with those of others, and mechanisms needed for successful coordination; and
- sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted.

To allow for more efficient efforts to assess portwide resilience, the Secretary of Homeland Security should direct the Assistant Secretary of Infrastructure Protection and the Commandant of the Coast Guard to look

for opportunities to collaborate to leverage existing tools and resources to conduct assessments of portwide resilience. In developing this approach, DHS should consider the use of data gathered through IP's voluntary assessments of port area critical infrastructure or regional RRAP assessments—taking into consideration the need to protect information collected voluntarily—as well as Coast Guard data gathered through its MSRAM assessments, and other tools used by the Coast Guard.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security for review and comment. In its written comments reprinted in appendix I, DHS concurred with both of our recommendations.

With regard to our first recommendation, that DHS develop an implementation plan for its forthcoming resilience policy, DHS stated that while its RIT has worked to draft a resilience policy including findings and policy statements from key strategic documents such as the QHSR, the department has yet to commence developing an implementation strategy. DHS also noted that it has undertaken a range of activities that support resilience and that further avenues—such as an implementation strategy—are under consideration. Developing an implementation strategy for its resilience policy that addresses the steps needed to achieve results; identifies entities responsible for implementing the policy, their roles, and coordination mechanisms; and determines the resources and investments associated with the strategy would address the intent of our recommendation.

With regard to our second recommendation, that DHS seek opportunities for IP and the Coast Guard to collaborate in assessing portwide resilience, DHS stated that the two components would work with ORP in defining their roles in contributing to port resilience. DHS also stated that the RIT would create a subcommittee this fiscal year to provide a forum for discussing the harmonization of resilience activities and programs across DHS. These proposed actions appear to be positive steps in enhancing IP and Coast Guard collaboration that would address the intent of this recommendation.

DHS provided technical comments, which we incorporated as appropriate. We are sending copies of this report to the Secretary of Homeland Security, applicable congressional committees, and other interested parties. This report is also available at no charge on GAO's website at http://www.gao.gov.

If you or your staffs have questions about this report, please contact me at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Appendix I: Comments from the Department of Homeland Security

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

Homeland Security

October 17, 2012

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

Re: Draft Report GAO-13-11, "CRITICAL INFRASTRUCTURE PROTECTION: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts Across Ports and Other Infrastructure"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgment that DHS has taken steps to emphasize the concept of resilience among its Components. Additionally, GAO found that DHS was developing or updating programs to assess vulnerability and risk at critical infrastructure facilities and within groups of related infrastructure, regions, and systems to place greater emphasis on resilience.

The draft report contained two recommendations directly involving DHS with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct the Assistant Secretary for Policy to develop an implementation strategy for this new policy that identifies the following characteristics and others that may be deemed appropriate:

- steps needed to achieve results, by developing priorities, milestones, and performance measures;
- responsible entities, their roles compared to others, and mechanisms needed for successful coordination; and
- sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted.

Response: Concur. The DHS Resilience Integration Team (RIT), the DHS-wide organization composed of subject matter experts on resilience, drafted and is considering a policy cataloguing what resilience means in the context of the Department. It includes key findings and policy statements from existing departmental and national strategies and policies, such as the National Security Strategy, the Quadrennial Homeland Security Review, and the National Strategy for Global Supply Chain Security. It is important to note that the RIT was formed to focus, share, and develop the numerous activities, policies, and views on resilience from across the Department, and to date, the development of an implementation strategy has yet to commence. Therefore, it is accurate to make a note of the wide range of past and present resilience activities, while also recognizing that several avenues remain in progress and under consideration (i.e., the viability of strategy development).

Recommendation 2: Direct the Assistant Secretary of Infrastructure Protection and Commandant of the Coast Guard to look for opportunities to collaborate and leverage existing tools and resources to conduct assessments of portwide resilience. In developing this approach, DHS should consider the use of data gathered through IP's voluntary assessments of port-area critical infrastructure or Regional Resiliency Assessment Program (RRAP) assessments – taking into consideration the need to protect information collected voluntarily – as well as Coast Guard data gathered through its Maritime Security Risk Analysis Model (MSRAM) assessments, and other tools used by the Coast Guard.

Response: Concur. The Coast Guard and the National Protection and Programs Directorate's Office of Infrastructure Protection will continue to work with the DHS Office of Resilience Policy on defining their role in the resilience of ports and contributing to this important function. The RIT will create a subcommittee in Fiscal Year 2013 to provide a forum for discussing the harmonization of resilience activities and programs across DHS, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-9610 or CaldwellS@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director, and Adam Couvillion, Analyst-in-Charge, managed this assignment. Adam Anguiano, Michele Fejfar, Eric Hauswirth, Tracey King, and Jessica Orr made significant contributions to the work.

Related GAO Products

Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act. GAO-12-1009T. Washington, D.C.: September 11, 2012.

Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments. GAO-12-378. Washington, D.C.: May 31, 2012.

Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response. GAO-12-494R. Washington, D.C.: April 6, 2012.

Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations. GAO-12-14. Washington, D.C.: November 17, 2011.

Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened. GAO-12-47. Washington, D.C.: November 17, 2011.

Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities. GAO-11-537R. Washington, D.C.: May 19, 2011.

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010.

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.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007.

Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery. GAO-07-412. Washington, D.C.: March 28, 2007.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. GAO-05-394. Washington, D.C.: April 15, 2005.