United States Government Accountability Office

Testimony

Before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, November 19, 2013

MARITIME SECURITY

Progress and Challenges in Key DHS Programs to Secure the Maritime Borders

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice Issues

November 19, 2013

MARITIME SECURITY

Progress and Challenges in Key DHS Programs to Secure the Maritime Borders

GAO Highlights

Highlights of GAO-14-196T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Maritime borders are gateways to our nation's maritime transportation system of ports, waterways, and vessels—which handle billions of dollars of cargo annually. An attack on this system could have dire consequences and affect the global economy. In addition, criminals could use small vessels to smuggle narcotics, aliens, and other contraband across U.S. maritime borders. Within DHS, the Coast Guard is responsible for many homeland security efforts in the maritime domain, including conducting port facility and commercial vessel inspections and coordinating maritime information-sharing efforts, among other things. In addition, CBP is responsible for screening incoming vessels' crews and cargoes to facilitate the flow of legitimate trade and passengers.

This testimony identifies key factors important to secure the maritime borders, and discusses progress and challenges in related DHS programs. This statement is based on products GAO issued from July 2003 through October 2013.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen its maritime security programs. DHS generally concurred with these recommendations and has taken actions, or has actions under way, to address them.

View GAO-14-196T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

GAO's prior work has identified several key factors important to secure the maritime borders. The Department of Homeland Security (DHS) and its components have made progress (e.g. coordinating with partners), and in some cases also experienced challenges, with their related maritime security programs.

- **Maintaining robust maritime domain awareness.** It is critical that federal agencies maintain maritime domain awareness—the understanding of anything associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of the United States. The U.S. Coast Guard has developed systems—including information-sharing and vessel-tracking systems—to enhance maritime domain awareness. GAO's prior work has found that Coast Guard has made progress in developing its systems but that it also experienced some challenges. For example, in July 2011, GAO reported that the Coast Guard had not met its goal of building a system intended to enable the sharing of information among its new offshore vessels and aircraft. GAO recommended that the agency take actions to address this challenge. DHS concurred and stated it planned to take actions.
- **Assessing risks coming from foreign ports.** The security of maritime borders also depends upon security at foreign ports where cargoes bound for the United States originate. U.S. Customs and Border Patrol (CBP) and the Coast Guard have developed models to assess the risks of foreign ports, foreign vessels entering U.S. ports, and the cargoes carried by these vessels from these ports. In September 2013, GAO found that CBP has taken steps to enhance the security of U.S.-bound cargo, but CBP does not periodically assess the supply chain security risks from foreign ports that ship cargo to the United States. GAO recommended that CBP periodically assess the supply chain security risks from these ports. DHS concurred with GAO's recommendation and reported that it planned to take actions to address it.
- **Conducting maritime surveillance, interdiction, and security operations.** Along the coasts and in ports, maritime surveillance, interdiction, and operations are conducted to ensure the security of the maritime borders. For example, CBP's Office of Air and Marine is to provide maritime surveillance and interdiction capabilities. In March 2012, GAO found that the office did not meet its national performance goal and did not provide higher rates of support in locations designated as high priority. GAO made recommendations to help ensure that the office's assets and personnel are best positioned to effectively meet mission needs and address threats, among other things. DHS concurred and reported that it planned to take action to address the recommendations by the end of March 2014.
- **Measuring performance.** In securing our maritime borders, DHS and its component agencies have faced challenges in developing meaningful performance measures. For example, GAO's prior work found that they have experienced challenges collecting complete, accurate, and reliable data; among other things. In January 2011, GAO reported that both CBP and the Coast Guard tracked the frequency of illegal seafarer incidents at U.S. seaports, but the records of these incidents varied considerably between the two component agencies and between the agencies' field and headquarters units. GAO made a recommendation to improve the accuracy of DHS data, and DHS concurred and has made progress in addressing the recommendation.

Chairman Miller, Ranking Member Jackson Lee, and Members of the Subcommittee:

Thank you for the opportunity to discuss key aspects of a secure maritime border. Maritime borders are gateways to our nation's maritime transportation system of ports, waterways, and vessels, which handle billions of dollars of cargo annually. Accordingly, maritime borders are critical to our national security. For instance, an attack on this system could have a widespread affect on global shipping, international trade, and the global economy, and an attack on a domestic port could have dire consequences because of the size of ports and their general proximity to metropolitan areas. Further, criminals could use small vessels to smuggle narcotics, aliens, and other contraband across U.S. maritime borders. Balancing maritime security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for the public and private sectors alike.

Within the Department of Homeland Security (DHS), the U.S. Coast Guard has much of the responsibility for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, the Coast Guard conducts port facility and commercial vessel inspections, coordinates maritime information-sharing efforts, and promotes maritime domain awareness, among other things.[1] Also within DHS, U.S. Customs and Border Protection (CBP) is responsible for screening incoming vessels' crews and cargoes for the presence of contraband, such as weapons of mass destruction, illicit drugs, or explosives, while facilitating the flow of legitimate trade and passengers. Several other DHS components, such as the Transportation Security Administration, the Domestic Nuclear Detection Office, and the

[1]Maritime domain awareness is the understanding by stakeholders involved in maritime security of anything associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of the United States.

Federal Emergency Management Agency, also have roles in securing our maritime borders.[2]

My statement today identifies key factors that are important to secure the maritime borders and discusses progress and challenges in related DHS programs. Specifically, I will address the following factors: (1) maritime domain awareness; (2) risks from foreign ports; (3) international partnerships in global supply chain security; (4) maritime surveillance, interdiction, and security operations; (5) partnerships and coordination along the coasts and in ports; and (6) measuring performance.

My statement is based on reports and testimonies we issued from July 2003 through October 2013 related to maritime, port, vessel, and cargo security and other related aspects of maritime border security. To perform the work for our previous reports and testimonies, we visited domestic and overseas ports; reviewed agency program documents, port security plans, and other documents; and interviewed officials from the federal, state, local, private, and international sectors, among other things. The officials we met with represented a wide variety of stakeholders including the Coast Guard, CBP, port authorities, terminal operators, vessel operators, foreign governments, and international trade organizations. Further details on the scope and methodology for the previously issued reports and testimonies are available within each of the published products. We conducted the work on which this statement is based 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[2]The Transportation Security Administration has responsibility for managing the Transportation Worker Identification Credential program, which is designed to control the access of maritime workers to regulated maritime facilities in the United States. The Domestic Nuclear Detection Office is responsible for acquiring and supporting the deployment of radiation detection equipment, including radiation portal monitors at domestic seaports to support the scanning of cargo containers before they enter U.S. commerce. The Federal Emergency Management Agency is responsible for administering grants intended to improve the security of the nation's highest-risk port areas.

Several Factors Are Important To Secure Maritime Borders and DHS Has Made Progress to Address Them, but Challenges Remain

Our prior work has identified several key factors important to securing the maritime borders, which include (1) maintaining robust maritime domain awareness, (2) assessing risks coming from foreign ports, (3) leveraging international partnerships, (4) conducting maritime surveillance, interdiction, and security operations, (5) coordinating with partners along the coast and in ports, and (6) measuring performance. Our prior work has also shown that DHS and its components have made progress, and in some cases experienced challenges, with their programs to address these factors.

Maintaining Robust Maritime Domain Awareness

To ensure the security of our maritime borders, it is critical that federal agencies maintain robust maritime domain awareness. According to the *National Plan to Achieve Maritime Domain Awareness*, the maritime domain provides an expansive pathway around the world that terrorist organizations could exploit for moving equipment and personnel, as well as a means for launching attacks. Timely awareness of the maritime domain and knowledge of threats helps the Coast Guard to detect, deter, interdict, and defeat adversaries. For example, according to the Coast Guard, maritime domain awareness played a key role in allowing it to interdict narcotics, intercept thousands of alien migrants, detain hundreds of suspected smugglers, board foreign vessels to suppress illegal fishing, and rescue thousands of people.

To enhance maritime domain awareness, the Coast Guard works with its maritime partners to facilitate the sharing and dissemination of a wide array of information and intelligence to better secure the nation's maritime transportation system against potential threats. The Coast Guard has made progress in developing its maritime domain awareness systems—including its Common Operational Picture—by increasing user access and adding data sources.[3] The Coast Guard also has other related systems that can be used to provide enhanced maritime domain information to other Coast Guard units and port partners. However, as we previously reported, the Coast Guard experienced challenges in developing and implementing these systems. For example, in July 2011, we reported that the Coast Guard had not met its goal of building a single,

[3]The Common Operational Picture is an interactive map-based information system that can be shared among Coast Guard commands.

fully interoperable Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance program system intended to enable the sharing of information among its new offshore vessels and aircraft.[4] In addition, in February 2012, we reported that the intended information-sharing capabilities of the Coast Guard's WatchKeeper software—which was designed to gather data to help port partner agencies collaborate in the conduct of operations and share information, among other things—met few port agency partner needs. This is in part because the agency did not determine these needs when developing the system.[5] Further, in April 2013, we reported that, among other things, the Coast Guard had not followed its own information technology development guidance when developing one of its new maritime domain awareness systems, known as Coast Guard One View.[6] We recommended, and the Coast Guard concurred, that the agency take actions to address these challenges. DHS stated that it planned to take actions to address these recommendations, such as developing necessary acquisition documentation.

In addition to its own systems, the Coast Guard also relies on systems operated by other entities to help it track vessels and enhance maritime domain awareness. For example, to track vessels at sea, the Coast Guard uses a long-range identification and tracking system and an automatic identification system that broadcasts information on the vessels and their locations, and to track vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system and also obtains information from radar and cameras in some ports. In March 2009, we reported on the challenges of tracking small vessels using available technologies.[7] For example, we reported that although the Coast Guard and other agencies may have technology systems that can track small vessels within some ports, these

[4]GAO, *Coast Guard: Action Needed as Approved Deepwater Program Remains Unachievable,* GAO-11-743 (Washington, D.C.: July 28, 2011).

[5]GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers,* GAO-12-202 (Washington, D.C: Feb. 13, 2012).

[6]GAO, *Coast Guard: Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program,* GAO-13-321 (Washington, D.C.: Apr. 25, 2013).

[7]GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed,* GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

did not always work in bad weather or at night. In September 2012, we reported that the expansion of vessel tracking to all small vessels may be of limited utility because of, among other things, the large number of small vessels, the difficulty in identifying threatening actions, and the challenges associated with getting resources on scene in time to prevent an attack once it has been identified.[8] DHS and its components—such as the Coast Guard and CBP—have started or completed initiatives to improve maritime domain awareness in order to address small vessel security risks, including an initiative to help CBP better track small vessels arriving from foreign locations and another initiative to assist the Coast Guard in assessing and monitoring small vessel launch sites.

Assessing Risks Coming from Foreign Ports

The security of maritime borders also depends, in part, upon security at foreign ports where cargo and vessels bound for the United States may originate. The CBP and Coast Guard have developed models to assess the risks of foreign ports, foreign vessels entering U.S. ports, and the cargo carried by these vessels. In particular, CBP developed the Container Security Initiative (CSI) program that places officials at select foreign ports to use intelligence and risk assessment information to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing weapons of mass destruction or other terrorist contraband.[9] CBP's selection of the initial 23 CSI ports in 2002 was primarily based on the volume of U.S.-bound containers, but beginning in 2003, CBP considered more threat information when it expanded the number of CSI ports.[10] In our September 2013 report, we reported that CBP had not assessed the risk posed by foreign ports that ship cargo to the United States since 2005.[11] In 2009, CBP developed a model that ranked 356 potential expansion ports for a related program on the basis of risk, but it was not implemented because of budget cuts. We

[8]GAO, *Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act,* GAO-12-1009T (Washington, D.C.: Sept. 11, 2012).

[9]As of July 2013, there were 58 CSI ports in 32 countries that, collectively, accounted for over 80 percent of the container shipments imported into the United States.

[10]We reported in September 2013 that CBP subsequently added 35 ports to the CSI program from 2003 through 2007 on the basis of additional criteria, such as strategic threat factors and diplomatic or political considerations.

[11]GAO, *Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports,* GAO-13-764 (Washington, D.C.: Sept. 16, 2013).

found in September 2013 that by applying CBP's risk model to fiscal year 2012 cargo shipment data, CSI did not have a presence at about half of the ports CBP considered high risk, and about one fifth of the existing CSI ports were at lower risk locations. As a result, we recommended that CBP periodically assess the supply chain security risks from foreign ports that ship cargo to the United States and use the results to inform any future expansion of CSI and determine whether changes need to be made to existing CSI ports. DHS concurred with our recommendation and reported that by December 2014 it plans to develop a process for conducting periodic assessments of the supply chain security risks from all ports that ship cargo to the United States and use information from the assessments to determine if future expansion or adjustments to CSI locations are appropriate.

While CBP is focused on the security of the cargo shipped to the United States from foreign ports, the Coast Guard is focused on the security of ports and the vessels arriving in the United States. Under the International Port Security program, Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established international standards. We reported in October 2007 that the Coast Guard had found that most of the over 100 countries it visited had substantially implemented international standards.[12] More recently, the Coast Guard reported in November 2013 that it had visited over 150 countries. In September 2012, we reported that the Coast Guard had made progress with implementing its International Port Security program despite a number of challenges.[13] For example, we reported that the Coast Guard was able to alleviate sovereignty concerns of some countries by including a reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit U.S. ports. Further, as we reported in September 2013, the Coast Guard developed a risk-informed model—that it updates annually—as part of its International Port Security program to regularly assess the potential threat foreign ports pose to the maritime supply chain and make operational decisions.[14] According to the Coast Guard *International Port Security Program: Annual Report 2012*, the Coast Guard uses the model to make informed decisions on how to

[12]GAO, *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later,* GAO-08-126T, (Washington, D.C.: Oct. 30, 2007).

[13]GAO-12-1009T.

[14]GAO-13-764.

engage each country with the International Port Security program, including (1) how often to visit ports, (2) how many staff to assign to a particular visit, and (3) whether the country requires assistance.[15]

In addition to assessing the security of foreign ports, the Coast Guard also uses the results of the International Port Security program to help determine which arriving foreign vessels to board and inspect through its Port State Control program. In particular, according to the Coast Guard's *International Port Security Program: Annual Report 2012*, the Coast Guard is to use risk-based criteria to identify which foreign vessels entering U.S. ports and waterways it considers to be at risk of noncompliance with international or domestic regulations, and perform compliance examinations of these vessels. The risk-based criteria used to make these decisions include the vessel's management, the flag state under which vessel is registered, and the vessel's security compliance history resulting from previous examinations.

Leveraging International Partnerships in Global Supply Chain Security

International partnerships based on international standards are another key aspect of a secure maritime border. For example, the International Ship and Port Facility Security (ISPS) Code was developed after the September 11, 2001, terrorist attacks to establish measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS Code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance based; therefore, compliance can be achieved through a variety of security measures. Additionally, in collaboration with 11 other members of the World Customs Organization, CBP developed the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), which is based in part on the core concepts of CBP programs and provides standards for collaboration among customs administrations and entities participating in the supply chain.[16] The SAFE Framework was adopted by the 173 World Customs Organization

[15] U.S. Coast Guard, *International Port Security Program: Annual Report 2012* (Washington, D.C.: Mar. 31, 2012).

[16]The World Customs Organization is an intergovernmental organization representing the customs administrations of 173 countries that aims to enhance the effectiveness and efficiency of customs administrations.

member customs administrations in June 2005; and as of our last report on this topic in July 2008, 154 had signed letters of intent to implement the standards.

CBP and the Coast Guard also leverage relationships with private industry stakeholders and foreign partners to promote the security of maritime borders, given that protecting domestic ports begins outside the United States where inbound shipments enter the supply chain. For example, the Customs-Trade Partnership Against Terrorism (C-TPAT) program is a voluntary program that enables CBP officials to work in partnership with private companies to review and approve the security of their international supply chains.[17] Companies that join the C-TPAT program commit to improving the security of their supply chains and agree to provide CBP with information on their specific security measures. In addition, the companies agree to allow CBP to verify, among other things, that their security measures meet or exceed CBP's minimum security requirements. This allows CBP to ensure that the security measures outlined in a member's security profile are in place and effective.[18] In April 2008, we reported that the C-TPAT program holds promise as part of CBP's multifaceted maritime security strategy.[19] We also reported that the program allows CBP to develop partnerships with the trade community, which is a challenge given the international nature of the industry and resulting limits on CBP's jurisdiction and activities, and provides CBP with a level of information sharing that would otherwise not be available. However, our reports raised concerns about the overall management of the program and challenges in verifying that C-TPAT members meet security criteria. We recommended that CBP strengthen program management by developing planning documents and performance measures, and by improving the process for validating

[17]In November 2001, CBP announced the C-TPAT program as part of its efforts toward facilitating the free flow of goods while ensuring that the containers do not pose a threat to homeland security. In October 2006, the Security and Accountability for Every Port Act of 2006 established a statutory framework for the C-TPAT program, codified its existing membership processes, and added new components—such as time frames for certifying, validating, and revalidating members' security practices. 6 U.S.C. §§ 961-973

[18]CBP has awarded initial C-TPAT certification—or acceptance of the company's agreement to voluntarily participate in the program—to over 10,000 companies, as of February 2012.

[19]GAO, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices,* GAO-08-240 (Washington, D.C.: Apr. 25, 2008).

security practices of C-TPAT members. CBP agreed with these recommendations and has addressed them.

Additionally, through mutual recognition arrangements with foreign partners, the security-related practices and programs established by the customs or maritime security administration of one partner are recognized and accepted by the administration of another.[20] Both CBP and the Coast Guard have entered into such arrangements. For example, CBP can expand the reach of its supply chain security programs (such as C-TPAT) through mutual recognition arrangements. According to the World Customs Organization, mutual recognition arrangements allow customs administrations to target high-risk shipments more effectively and expedite low-risk shipments by, for example, reducing redundant examinations. As we reported in September 2013, mutual recognition arrangements may allow the Coast Guard to allocate resources more efficiently and reduce risks.[21] For example, we further reported that the Coast Guard signed a memorandum of understanding with the European Union that establishes a process for mutually recognizing security inspections of each other's ports.[22] According to DHS documents and Coast Guard officials in Europe, by signing this memorandum of understanding, the Coast Guard plans to reassign some International Port Security officials from Europe to Africa, where certain countries are having more difficulties than others in implementing effective antiterrorism measures in their ports. Further, we reported that one trade-off of signing the memorandum of understanding is that Coast Guard's International Port Security officials will not have the same opportunities to have face-to-face interactions and share port security information and practices directly with their European Union counterparts as in the past. Despite this trade-off, Coast Guard officials stated that entering into such

[20]Mutual recognition arrangements can be entered into with other countries as well as other governing bodies, such as the European Union. For the purposes of this testimony, the countries and governing bodies that enter into mutual recognition arrangements with the United States are considered partners.

[21]GAO-13-764.

[22]According to DHS officials, the European Union characterizes its port visits as "inspections." Under the memorandum of understanding procedures, the Coast Guard recognizes a successful European Union inspection of its member states' ports in the same manner as it would recognize a successful country visit by Coast Guard inspectors. Coast Guard officials stated that they have collaborated with their European counterparts to develop standard operating procedures for these port inspections.

arrangements increases efficiencies and noted that they intend to negotiate additional memorandums of understanding with other foreign governments that have strong port inspection programs.

Conducting Maritime Surveillance, Interdiction, and Security Operations along the Coast and in Ports

Along the coast and in ports, maritime surveillance, interdiction, and security operations are conducted to ensure the security of maritime borders. For example, CBP's Office of Air and Marine provides maritime surveillance and interdiction capabilities. Its strategic assumptions include the ability to provide a 24-hour, 7-day a week response to border penetrations anywhere along the U.S. border, with a 1-hour response time for areas designated as high priority.[23] We reported in March 2012 that as of May 2011, the Office of Air and Marine had placed about half of its air assets on the southwest border region and the remainder in the northern and southeast regions, while marine resources were distributed fairly evenly across the northern, southwest, and southeast regions.[24] Further, our analysis of the Office of Air and Marine's fiscal year 2010 performance results indicate that they did not meet their national performance goal to fulfill greater than 95 percent of Border Patrol air support requests and did not provide higher rates of support in locations designated as high priority based on threats. We made recommendations to help ensure that the Office of Air and Marine's assets and personnel are best positioned to effectively meet mission needs and address threats, and to help DHS better leverage existing resources, eliminate unnecessary duplication, and enhance efficiencies. DHS concurred with these recommendations, and described actions it was taking, or planned to take to address them, including making strategic and technological changes in its assessment of the mix and placement of its resources by the end of March 2014.

[23]CBP's Office of Air and Marine resources are divided among 70 air and marine locations across three regions (southeast, southwest, and northern); the National Capital area; and National Air Security Operations Centers throughout the continental United States, Puerto Rico, and the U.S. Virgin Islands. In deciding how resources should be allocated, considerations include historical location, congressional direction, and differences in geography and relative need for air and marine support to address threats.

[24]The Office of Air and Marine has 23 branches and 6 National Air Security Operations Centers across these regions, and within the branches, the office may have one or more air or marine units. See GAO, *Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets*, GAO-12-518 (Washington, D.C.: Mar. 30, 2012).

In addition to CBP's Office of Air and Marine interdiction and response activities, the Coast Guard conducts a number of activities to deter potential threats to the United States' maritime borders. For example, the Coast Guard escorts a certain percentage of high-capacity passenger vessels—cruise ships, ferries, and excursion vessels—and energy commodity tankers to protect against an external threat, such as a waterborne improvised explosive device. The Coast Guard also provides additional security response capabilities through its Maritime Safety and Security Teams and Maritime Security Response Teams. Created by the Maritime Transportation Security Act of 2002, the Maritime Safety and Security Teams constitute a maritime security antiterrorism force.[25] The teams are managed as assets that may be deployed nationwide, and are responsible for safeguarding the public and protecting vessels, harbors, ports, facilities, and cargo in U.S. territorial waters. The teams are to maintain readiness to deploy to events such as terrorist threats or incidents and storm recovery operations, and routinely deploy to national special security events such as the Super Bowl and the presidential inauguration. They are also to enforce security zones around high-interest vessels in transit and at other times when additional levels of security are needed within the nation's ports and waterways. The Coast Guard's Maritime Security Response Team complements the Maritime Security and Safety Team, and is charged with maintaining a high readiness posture 365 days a year. The Maritime Security Response Team is the Coast Guard's advanced interdiction force for counterterrorism and law enforcement operations of a high-risk nature. The team provides a variety of advanced capabilities or skills, including addressing threats posed by weapons of mass destruction and vertically deploying from helicopters to engage potentially hostile personnel.

Coordinating with Partners along the Coast and in Ports

Along the coast and in ports, partnerships and coordination among various stakeholders contribute to the security of the maritime borders. To target the threat of transnational terrorist and criminal acts along the coastal borders, the Maritime Operations Coordination Plan, established in 2011, directs CBP, Coast Guard, and U.S. Immigration and Customs Enforcement's Homeland Security Investigations to utilize the fusion of their intelligence, planning, and operations capabilities through the

[25]See 46 U.S.C. § 70106.

formation of Regional Coordinating Mechanisms.[26] The Coast Guard serves as the lead agency responsible for planning and coordinating among components. We reported in September 2013 that, according to the Coast Guard, there were 32 Regional Coordinating Mechanisms as of June 2013 that aligned with Coast Guard sectors' geographic areas of responsibility.[27] In addition to the lead agencies, other stakeholders include the Federal Bureau of Investigation; the Drug Enforcement Administration; the U.S. Attorney's Office; state, local, and tribal law enforcement agencies; and foreign law enforcement agencies.

In ports, Area Maritime Security Committees consist of key stakeholders who (1) may be affected by security policies and (2) share information and develop port security plans. These committees, which are required by Coast Guard regulations that implement the Maritime Transportation Security Act of 2002, also identify critical port infrastructure and risks to the port, develop mitigation strategies for these risks, and communicate appropriate security information to port stakeholders.[28] Recommended committee members include a diverse array of port stakeholders, including federal, state, and local agencies, as well as private sector entities such as terminal operators, yacht clubs, shipyards, marine exchanges, commercial fishermen, trucking and railroad companies, organized labor, and trade associations. Area Maritime Security Committees also are to serve as forums for developing Area Maritime Security Plans. The Maritime Transportation Security Act of 2002 required the Coast Guard to develop Area Maritime Security Plans—to be updated every 5 years—for ports throughout the nation.[29] The Coast Guard develops these plans for each of the 43 geographically defined port areas with input from applicable governmental and private entities, and the plans are to serve as the primary means to identify and coordinate Coast

[26]The Maritime Operations Coordination Plan was signed by the Director of Homeland Security Investigations, the Commissioner of CBP, and the Commandant of the Coast Guard.

[27]GAO, *Department of Homeland Security: Opportunities Exist to Enhance Visibility over Collaborative Field Mechanisms*, GAO-13-734 (Washington, D.C.: Sept. 27, 2013).

[28]33 C.F.R. §§ 103.300-.310.

[29]46 U.S.C. § 70103(b)(2)(G). In 2006, the Security and Accountability for Every Port Act (SAFE Port Act) added a requirement that AMSPs include recovery issues by identifying salvage equipment able to restore operational trade capacity (46 U.S.C. § 70103(b)(2)(G)).

Guard procedures related to prevention, protection, and security. In March 2007, we reported that there was a wide variance in ports' natural disaster planning efforts and that Area Maritime Security Plans—limited to security incidents—could benefit from unified planning to include an all-hazards approach. We recommended that DHS encourage port stakeholders to use existing forums for discussing all-hazards planning.[30] DHS concurred with our recommendation and implemented it through the fiscal year 2007 Port Security Grant Program supplemental program, which was designed in part to facilitate the development of a Port-Wide Risk Management/Mitigation and Business Continuity/Resumption of Trade Plan.[31]

Measuring Maritime Security

Another important aspect of a secure border is measuring maritime security. In the component agencies' implementation of the various maritime security related programs I have described today and as we have previously reported, one of the challenges that DHS and its component agencies have faced has been the lack of adequate performance measures. The following are some of the performance measurement challenges we have reported on:

- *Lack of reliable and accurate data*: DHS and its component agencies have experienced challenges collecting complete, accurate, and reliable data. For example, in January 2011, we reported that both CBP and the Coast Guard tracked the frequency of illegal seafarer incidents at U.S. seaports, but the records of these incidents varied considerably between the two component agencies and between the agencies' field and headquarters units.[32] As a result, the data DHS

[30]46 U.S.C. § 70103(b). GAO, *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery*. GAO-07-412 (Washington, D.C.: Mar. 28, 2007).

[31]Fiscal year 2007 Port Security Grant Program supplemental program funding supports the development of a plan that emphasizes port-wide partnerships, regional management of risk, and business continuity/resumption of trade. The central plan focuses on security across the port area and articulates a strategy for ensuring business continuity and resumption of trade within the port in the event of an emergency.

[32]Illegal seafarers include both absconders (seafarers CBP has ordered detained on-board a vessel in port, but who depart a vessel without permission) and deserters (seafarers CBP grants permission to leave a vessel, but who do not return when required). GAO, *Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened*, GAO-11-195 (Washington D.C.: Jan. 14, 2011).

used to inform its strategic and tactical plans were of undetermined reliability. We recommended that CBP and the Coast Guard determine why their data varied and jointly establish a process for sharing and reconciling records of illegal seafarer entries at U.S. seaports. DHS concurred and has made progress in addressing the recommendation.

- *Not using data to manage programs*: DHS and its component agencies have not always had or used performance information to manage their missions. For example, we reported in February 2008 that Coast Guard officials used their Maritime Information for Safety & Law Enforcement database—Coast Guard's primary data system for documenting facility inspections and other activities—to review the results of inspectors' data entries for individual maritime facilities, but the officials did not use the data to evaluate the facility inspection program overall.[33] We found that a more thorough evaluation of the facility compliance program could provide information on, for example, the variations we identified between Coast Guard units in oversight approaches, the advantages and disadvantages of each approach, and whether some approaches work better than others. We recommended that Coast Guard assess its Maritime Information for Safety & Law Enforcement compliance data, including the completeness and consistency of the data and data field problems, and make any changes needed to more effectively utilize the data. Coast Guard agreed and has reported taking actions to address the recommendation. These actions include hiring a full-time management and program analyst to consistently review the data for trends and gaps, and developing training resources, help desks, and conferences, among other things, to help field personnel track changes to Maritime Information for Safety & Law Enforcement and to improve data entry time and consistency.

- *Lack of outcome-based performance measures*: DHS and its component agencies have also experienced difficulties developing and using performance measures that focus on outcomes. Outcome-based performance measures describe the intended result of carrying out a program or activity. For example, although CBP had performance measures in place for its C-TPAT program, these

[33]GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data,* GAO-08-12 (Washington, D.C.: Feb. 14, 2008).

measures focused on program participation and facilitating trade and travel and not on improving supply chain security, which is the program's purpose. We made separate but related recommendations in July 2003, March 2005, and April 2008 that CBP develop outcome-based performance measures for this program.[34] CBP concurred, and, in response to our recommendations, identified measures to quantify actions required and to gauge C-TPAT's impact on supply chain security. The Coast Guard has faced similar issues with developing and using outcome-based performance measures. For example, we reported in November 2011 that the Coast Guard developed a measure to report its performance in reducing maritime risk, but faced challenges using this measure to inform decisions.[35] The Coast Guard reported it has improved the measure to make it more valid and reliable and stated it believes it is a useful proxy measure of performance, but notes that developing outcome-based performance measures is challenging because of limited historical data on maritime terrorist attacks.

Chairman Miller, Ranking Member Jackson Lee, and members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

[34]See GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (Washington, D.C.: Jul. 25, 2003); *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 11, 2005); and *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, GAO-08-240 (Washington, D.C.: Apr. 25, 2008).

[35]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).

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen L. Caldwell 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 statement. Individuals making key contributions to this statement include Christopher Conrad (Assistant Director), Tracey Cross, Christine Hanson, and Jeff Jensen.