United States Government Accountability Office

GAO

Testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Wednesday, July 21, 2010

MARITIME SECURITY

DHS Progress and Challenges in Key Areas of Port Security

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

July 21, 2010

MARITIME SECURITY

DHS Progress and Challenges in Key Areas of Port Security

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-940T, a testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

Ports, waterways, and vessels handle more than $700 billion in merchandise annually, and an attack on this system could have a widespread impact on global trade and the economy. Within the Department of Homeland Security (DHS), component agencies have responsibility for securing the maritime environment. The U.S. Coast Guard is responsible for protecting, among other things, U.S. economic and security interests in any maritime region. U.S. Customs and Border Protection (CBP) is responsible for keeping terrorists and their weapons out of the United States, securing and facilitating trade, and cargo container security. This testimony discusses DHS and its component agencies' progress, and challenges remaining, regarding (1) strengthening risk management (a strategy to help policymakers make decisions about assessing risks, allocating resources, and acting under conditions of uncertainty), (2) reducing the risk of small-vessel (watercraft less than 300 gross tons used for recreational or commercial purposes) threats, (3) implementing foreign port assessments, and (4) enhancing supply chain security. This statement is based on GAO products issued from December 2005 through June 2010, including selected updates conducted in July 2010.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen port security. DHS generally concurred.

View GAO-10-940T or key components.
For more information, contact Stephen L. Caldwell at (202) 512-8777 or CaldwellS@gao.gov.

What GAO Found

DHS and its component agencies have strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. In December 2005, GAO reported that while the Coast Guard had made progress in strengthening risk management by conducting risk assessments, those assessments were limited because they could not compare and prioritize relative risks of various infrastructures across ports. Since that time, the Coast Guard developed a risk assessment model designed to capture the security risk facing different types of targets, and allowing comparisons among targets and at the local, regional, and national levels. The Coast Guard uses the model to help plan and implement its programs and focus security activities where it believes the risks are greatest.

DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels but they face ongoing challenges. GAO reported from 2007 through 2010 that DHS and the Coast Guard have (1) developed a strategy to mitigate vulnerabilities associated with waterside attacks by small vessels; (2) conducted community outreach to encourage boaters to share threat information; (3) initiated actions to track small vessels; (4) tested equipment for detecting nuclear material on small vessels; and (5) conducted security activities, such as vessel escorts. However, the Coast Guard faces challenges with some of these efforts. For example, vessel tracking systems generally cannot track small vessels and resource constraints limit the Coast Guard's ability to meet security activity goals.

DHS and the Coast Guard developed the International Port Security Program in April 2004 to assess the security of foreign ports, but challenges remain in implementing the program. GAO reported in October 2007 that Coast Guard officials stated that there is reluctance by certain countries to allow the Coast Guard to visit their ports due to concerns over sovereignty. Also, the Coast Guard lacks the resources to assist poorer countries. Thus the Coast Guard is limited in its ability to help countries enhance their established security requirements. To overcome this, officials have worked with other federal agencies and international organizations to secure funding for training and assistance to countries that need to strengthen port security efforts.

DHS and CBP established the Secure Freight Initiative (SFI) to test the feasibility of scanning 100 percent of U.S.-bound cargo containers, but face challenges expanding the program. In October 2009, GAO reported that CBP has made progress in working with the SFI ports to scan U.S.-bound cargo containers; but because of challenges implementing scanning operations, such as equipment breakdowns, the feasibility of scanning 100 percent of U.S.-bound cargo containers remains largely unproven. At the time, CBP officials expressed concern that they and the participating ports could not overcome the challenges. GAO recommended that DHS conduct a feasibility analysis. DHS concurred with our recommendation, but has not yet implemented it.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss port security issues and their related challenges. 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 an attack on this system could have a widespread impact on global shipping, international trade, and the global economy. Balancing 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 DHS, component agencies have responsibility for securing the maritime environment. The U.S. Coast Guard is responsible for protecting the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including America's coasts, ports, and inland waterways. U.S. Customs and Border Protection (CBP) is responsible for keeping terrorists and their weapons out of the United States, securing and facilitating trade, and cargo container security.

Various laws have been enacted since the September 11, 2001 terrorist attacks to strengthen port security. The Homeland Security Act of 2002[1] charges DHS with establishing a risk management framework across the federal government to protect the nation's critical infrastructure and key resources. In addition, much of a new port security framework was set in place by the Maritime Transportation Security Act of 2002 (MTSA).[2] Enacted in November 2002, MTSA was designed, in part, to help protect the nation's ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; and (3) establishing a process to assess foreign ports from which vessels depart on voyages to the United States. The Security and Accountability For Every (SAFE) Port Act of 2006 later directed the Secretary of Homeland Security to, among other things, increase the security of container cargo bound for the United States by requiring CBP to establish a pilot program to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.[3] Further, in August 2007, the Implementing

[1]Pub. L. No. 107-296, § 201, 116 Stat. 2135, 2144 (2002).

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

[3]Pub. L. No. 109-347, § 231, 120 Stat. 1884, 1915-16 (2006).

Recommendations of the 9/11 Commission Act were enacted and provide, among other things, that by July 2012, a container loaded on a vessel in a foreign port shall not enter the United States unless that container is scanned before it is loaded onto the vessel.[4]

My statement today is based on related GAO reports and testimonies issued from December 2005 through June 2010 addressing risk management and port security, and also includes selected updates—conducted in July 2010—to the information provided in these products and on the actions agencies have taken to address recommendations made in these products that are also discussed in this statement. These products include our assessment of the progress that DHS and its component agencies have made to strengthen port security, the challenges that remain, and recommendations for improvement.[5] The details on the scope and methodology for those reviews are available in our published products. The selected updates include a review of (a) the Coast Guard's and CBP's fiscal year 2011 congressional budget justification and (b) CBP's fiscal year 2010 Report to Congress on supply chain security. In particular, my statement addresses the extent to which DHS and its component agencies have made progress and face challenges regarding (1) strengthening risk management, (2) reducing the risk of small-vessel threats,[6] (3) implementing foreign port assessments, and (4) enhancing supply chain security. We conducted this work in accordance with generally accepted government auditing standards.

In summary, DHS and its components agencies—the Coast Guard and CBP—have taken various actions to implement port security legislation and enhance port security. These efforts include (1) the Coast Guard's development of a risk assessment model to help prioritize limited resources; (2) DHS and the Coast Guard's development of a strategy and programs to reduce the risks associated with small vessels, such as a community outreach program, vessel tracking systems, and security

[4]Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007). The law defines scanning to be an examination with both nonintrusive imaging equipment and radiation detection equipment. In addition, while the law states that cargo containers are not to enter the United States unless they were scanned at a foreign port, actual participation in the program by sovereign foreign governments and ports is voluntary.

[5]See the list of related GAO products at the end of this statement.

[6]According to DHS's *Small Vessel Security Strategy*, "small vessels" are characterized as any watercraft—regardless of method of propulsion—less than 300 gross tons, and used for recreational or commercial purposes.

operations; (3) the Coast Guard's implementation of the International Port Security Program to assess security measures in foreign ports; and (4) CBP's efforts to scan U.S.-bound cargo containers. Although these initiatives have helped to improve port security, challenges remain, including resource constraints; the lack of technology to track and identify small vessels; sovereignty concerns over the Coast's Guard's visits to foreign ports; and a variety of political, logistical, and technological barriers to scanning all cargo containers. We have made recommendations to DHS in prior reports to help address these challenges, and DHS generally concurred with our recommendations in these reports.

The Coast Guard Has Made Progress in Improving Its Risk Management

In December 2005, we reported that risk management, a strategy for helping policymakers make decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty, had been endorsed by Congress and the President as a way to strengthen the nation against possible terrorist attacks against ports and other infrastructure.[7] Risk management has long been used in such areas as insurance and finance, but at the time its application to domestic terrorism had no precedent. We noted that unlike storms and accidents, terrorism involves an adversary with deliberate intent to destroy, and the probabilities and consequences of a terrorist act are poorly understood and difficult to predict. The size and complexity of homeland security activities and the number of organizations involved—both public and private—add another degree of difficulty to the task.

We have examined Coast Guard efforts to implement risk management for a number of years, noting how the Coast Guard's risk management framework developed and evolved. In 2005 we reported that of the three components GAO reviewed—the Coast Guard, the Office for Domestic Preparedness (this office's function is now within the Federal Emergency Management Agency), and the Information Analysis and Infrastructure Protection Directorate (now the National Protection and Preparedness Directorate)—the Coast Guard had made the most progress in establishing a foundation for using a risk management approach. While the Coast

[7]GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

Guard had made progress in all five risk management phases,[8] its greatest progress had been made in conducting risk assessments—that is, evaluating individual threats, the degree of vulnerability in maritime facilities, and the consequences of a successful attack.[9] However, we reported that those assessments were limited because they could not compare and prioritize relative risks of various infrastructures across ports. At the time the Coast Guard had actions under way to address the challenges it faced in each risk management phase and we did not make recommendations in those areas where the Coast Guard had actions well under way. Several of these actions were based, in part, on briefings GAO held with agency officials. Our recommendations were designed to spotlight those areas in which additional steps were most needed to implement a risk management approach to Coast Guard port security activities. We recommended that the Coast Guard take action to:

- establish a stronger linkage between local and national risk assessment efforts—an action that could involve, for example, strengthening the ties between local assessment efforts, such as area maritime security plans, and national risk assessment activities; and
-
- ensure that procedures for evaluating alternatives and making management decisions consider the most efficient use of resources—actions that could entail, for example, refining the degree to which risk management information is integrated into the annual cycle of program and budget review.

Since we made those recommendations, both DHS and the Coast Guard have made progress implementing a risk management approach toward

[8]The five phases of the risk management framework developed by GAO are (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and results achieved.

[9]Risk assessment is a function of (1) threat—the likelihood that a particular asset, system, or network will suffer an attack or an incident; (2) vulnerability—the likelihood that a characteristic of, or flaw in, an asset's, system's, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and (3) consequence—the negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

critical infrastructure protection. In 2006, DHS issued the National Infrastructure Protection Plan (NIPP), which is DHS's base plan that guides how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across each critical infrastructure sector in an integrated and coordinated fashion.[10] In 2009, DHS updated the NIPP to, among other things, increase its emphasis on risk management, including an expanded discussion of risk management methodologies and discussion of a common risk assessment approach that provided core criteria for these analyses.[11] For its part, the Coast Guard has made progress assessing risks and integrating the results of its risk management efforts into resource allocation decisions. Regarding risk assessments, the Coast Guard transitioned its risk assessment model from the Port Security Risk Assessment Tool (PS-RAT) to the Maritime Security Risk Assessment Model (MSRAM). In 2005 we reported that the PS-RAT was designed to allow ports to prioritize resource allocations within, not between, ports to address risk most efficiently. However, the new MSRAM can assess risk across ports and is used by every Coast Guard unit and assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios; that is, it combines potential targets with different means of attack, as recommended by the NIPP. The Coast Guard uses the model to help implement its strategy and concentrate maritime security activities when and where relative risk is believed to be the greatest. According to the Coast Guard, the model's underlying methodology is designed to capture the security risk facing different types of targets, allowing comparison between different targets and geographic areas at the local, regional, and national levels. We have also reported that the Federal Emergency Management Agency has included MSRAM results in its Port Security Grant Program guidelines as one of the data elements included in

[10]Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Homeland Security Presidential Directive 7 divided up the critical infrastructure in the United States into 17 industry sectors, such as transportation, energy, and communications, among others. In 2008, DHS established an 18th sector—Critical Manufacturing.

[11]The framework for the updated NIPP includes six components: (1) set goals and objectives; (2) identify assets, systems, and networks; (3) assess risks; (4) prioritize; (5) implement programs; and (6) measure effectiveness. 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).

determining grant awards to assist in directing grants to the ports of greatest concern or at highest risk.

With regard to the integration of risk management results into the consideration of risk mitigation alternatives and the management selection process, Coast Guard officials stated that the Coast Guard uses MSRAM to inform allocation decisions, such as the deployment of local resources and grants. We have also reported that at the national level, the Coast Guard uses MSRAM results for (1) long-term strategic resource planning, (2) identifying capabilities needed to combat future terrorist threats, and (3) identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that results are used to refine the Coast Guard's requirements for the number of required vessel escorts and patrols of port facilities. At the local level, the Captain of the Port[12] can use MSRAM as a tactical planning tool. The model can help identify the highest risk scenarios, allowing the Captain of the Port to prioritize needs and better deploy security assets.[13] The 2011 Congressional Budget Justification showed that the Coast Guard uses risk or relative risk to direct resources to the mitigation of the highest risk. For example, the use of risk management in the allocation of resources that is specific to port security concerns the Ports, Waterways, and Coastal Security program. This program has a performance goal to manage terror-related risk in the U.S. Maritime Domain to an acceptable level. The Coast Guard uses a program measure to direct resources to the programs that reduce risk the most based on the amount invested. Based on the development of the MSRAM assessment process and the use of risk management analysis results in its allocation of resources, we believe that the Coast Guard has addressed the recommendations discussed earlier concerning risk management.[14]

[12]The Captain of the Port is the Coast Guard officer designated by the Commandant of the Coast Guard to enforce within his or her respective areas port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

[13]For more information on the use of MSRAM see GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010).

[14]We have work planned for this committee to address a request concerning port security planning that will include a more detailed examination of MSRAM.

DHS and the Coast Guard Have Taken Several Actions to Address the Small-Vessel Threat but Challenges Remain in Mitigating the Risk

In recent years, we reported that concerns had arisen about the security risks posed by small vessels. In its April 2008 Small Vessel Security Strategy, DHS identified the four gravest risk scenarios involving the use of small vessels for terrorist attacks, which include the use of a small vessel as (1) a waterborne improvised explosive device, (2) a means of smuggling weapons into the United States, (3) a means of smuggling humans into the United States, and (4) a platform for conducting a stand-off attack—an attack that uses a rocket or other weapon launched at a sufficient distance to allow the attackers to evade defensive fire.[15] According to the Commandant of the Coast Guard, small vessels pose a greater threat than shipping containers for nuclear smuggling.[16] Some of these risks have been shown to be real through attacks conducted outside U.S. waters, but—as we reported in December 2009—no small-vessel attacks have taken place in the United States. Many vessels frequently travel among small vessels that operate with little scrutiny or notice, and some have suffered waterborne attacks overseas by terrorist or pirates who operated from small vessels. For example, at least three cruise ships have been attacked by pirates on small boats while armed with automatic weapons and rocket propelled grenades, although the three vessels were able to evade the pirates by either maneuvering or fighting back.[17] Oil tankers have also been attacked. For example, in October 2002, a small vessel filled with explosives rammed the side of an oil tanker off the coast of Yemen.[18] The concern about small-vessel attacks is exacerbated by the fact that some vessels, such as cruise ships, sail according to precise schedules and preplanned itineraries that could provide valuable information to terrorists in preparing for and carrying out an attack against a vessel.

DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels; however, they face ongoing

[15]Department of Homeland Security, *Small Vessel Security Strategy* (Washington, D.C., April 2008).

[16]From testimony delivered by Vice Admiral Thad Allen, Chief of Staff, United States Coast Guard, during a hearing on the Coast Guard role in border and maritime security, before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. Senate (Apr. 6, 2006).

[17]For more information on cruise ship security, see GAO-10-400.

[18]GAO, *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers*, GAO-08-141 (Washington, D.C.: December 10, 2007).

challenges related to some of these efforts. The following discusses some of our key findings with regard to reducing the risks associated with small vessels.

- **Small Vessel Security Strategy.** DHS released its Small Vessel Security Strategy in April 2008 as part of its effort to mitigate the vulnerability of vessels to waterside attacks from small vessels, and the implementation plan for the strategy is under review. According to the strategy, its intent is to reduce potential security and safety risks posed by small vessels through operations that balance fundamental freedoms, adequate security, and continued economic stability.[19] After review by DHS, the Coast Guard, and CBP, the draft implementation plan was forwarded to the Office of Management and Budget in April 2010, but the release of the plan has not been approved by the Office of Management and Budget.

- **Community Outreach.** Consistent with the Small Vessel Security Strategy's goal to develop and leverage strong partnerships with the small-vessel community, the Coast Guard, as well as other agencies—such as the New Jersey State Police, have several outreach efforts to encourage the boating community to share threat information; however, the Coast Guard program faces resource limitations. For example, the Coast Guard's program to conduct outreach to the boating community for their help in detecting suspicious activity, America's Waterway Watch, lost the funding it received through a Department of Defense readiness training program for military reservists in fiscal year 2008. Now it must depend on the activities of the Coast Guard Auxiliary, a voluntary organization, for most of its outreach efforts. In addition to America's Waterway Watch, the Coast Guard piloted a regional initiative—Operation Focused Lens—to increase public awareness of suspicious activity in and around U.S. ports, and direct additional resources toward gathering information about the most likely points of origin for an attack, such as marinas, landings, and boat ramps. According to Coast Guard officials, the agency views Operation Focused Lens to be a best practice, and the agency is considering plans to expand the program or integrate it into other existing programs.

[19]The goals of the Small Vessel Security Strategy are to (1) develop and leverage a strong partnership with the small-vessel community and public and private sectors; (2) enhance maritime security and safety; (3) leverage technology to enhance the ability to detect, determine intent, and when necessary, interdict small vessels; and (4) enhance coordination, cooperation, and communications between federal, state, local, and tribal stakeholders, the private sector, and international partners.

- **Vessel Tracking.** In December 2009, we reported that the Coast Guard was implementing two major unclassified systems to track a broad spectrum of vessels; however, these systems generally could not track small vessels.[20] The Coast Guard and other agencies have other technology systems, though—including cameras and radars—that can track small vessels within ports, but these systems were not installed at all ports or did not always work in bad weather or at night. Even with systems in place to track small vessels, there was widespread agreement among maritime stakeholders that it is very difficult to detect threatening activity by small vessels without prior knowledge of a planned attack.

- **Nuclear Material Detection Efforts.** DHS has developed and tested equipment for detecting nuclear material on small vessels; however, efforts to use this equipment in a port area have been limited to pilot programs. DHS is currently conducting 3-year pilot programs to design, field test, and evaluate equipment and is working with CBP, the Coast Guard, state, local, tribal officials, and others as they develop procedures for screening. These pilot programs are scheduled to end in 2010, when DHS intends to decide the future path of screening of small vessels for nuclear and radiological materials. According to DHS officials, initial feedback from federal, state, and local officials involved in the pilot programs has been positive. DHS hopes to sustain the capabilities created through the pilot programs through federal grants to state and local authorities through the port security grant program.[21]

- **Security Activities.** The Coast Guard also conducts various activities to provide waterside security including boarding vessels, escorting vessels into ports, and enforcing fixed security zones, although they are not always able to meet standards related to these activities. Through its Operation Neptune Shield, the Coast Guard sets the standards for local Coast Guard units to meet for some of these security activities. Although the Coast Guard units may receive some assistance from other law enforcement agencies in carrying out these security activities, Coast Guard data indicates that some units are not able to meet these standards due to resource constraints. However, the Coast Guard's guidance allows the Captain of the Port the latitude to shift resources to other priorities when

[20]For more information on vessel tracking systems, see 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).

[21]For more information, see GAO, *Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps*, GAO-10-883T (Washington, D.C.: June 30, 2010).

deemed necessary, for example when resources are not available to fulfill all missions simultaneously. The planned decommissioning of five Maritime Safety and Security Teams—a domestic force for mitigating and responding to terrorist threats or incidents—may continue to strain Coast Guard resources in meeting security requirements. Although remaining teams are to maintain readiness to respond to emerging events and are to continue performing routine security activities, such as vessel escorts, their ability to support local units in meeting operational activity goals may be diminished.

The Coast Guard Has a Program in Place to Assess the Security of Foreign Ports, but Challenges Remain in Implementing the Program

The security of domestic ports also depends upon security at foreign ports where cargoes bound for the United States originate. To help secure the overseas supply chain, MTSA required the Coast Guard to assess security measures in foreign ports from which vessels depart on voyages to the United States and, among other things, recommend steps necessary to improve security measures in those ports. In response, the Coast Guard established a program, called the International Port Security Program, in April 2004. Under this program, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code.[22] Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at such foreign ports at least once every 3 years.

As we reported in October 2007, Coast Guard officials told us that challenges exist in implementing the International Port Security Program.[23] Reluctance by some countries to allow the Coast Guard to visit

[22]The International Port Security Program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's antiterrorism measures in a port. The code was developed after the September 11 attacks and established 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.

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

their ports due to concerns over sovereignty was a challenge cited by program officials in completing their first round of port visits. According to these officials, before permitting Coast Guard officials to visit their ports, some countries insisted on visiting and assessing a sample of U.S. ports. The Coast Guard was able to accommodate their request through the program's reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit U.S. ports and observe ISPS Code implementation in the United States. This subsequently helped gain the cooperation of the countries in hosting a Coast Guard visit to their own ports. However, as Coast Guard program officials stated, sovereignty concerns may still be an issue, as some countries may be reluctant to host a comprehensive country visit on a recurring basis because they believe the frequency is too high.

Another challenge program officials cited is having limited ability to help countries build on or enhance their capacity to implement the ISPS Code requirements. Program officials stated that while their visits provide opportunities for them to identify potential areas to improve or help sustain the security measures put in place, other than sharing best practices or providing presentations on security practices, the program does not currently have the resources to directly assist countries, particularly those that are poor, with more in-depth training or technical assistance. To overcome this, program officials have worked with other agencies (e.g., the Departments of Defense and State) and international organizations (e.g., the Organization of American States) to secure funding for training and assistance to countries where port security conferences have been held (e.g., the Dominican Republic and the Bahamas).

CBP Has Established a Program to Scan U.S.-Bound Cargo Containers, but Challenges to Expanding the Program Remain

Another key concern in maritime security is the effort to secure the supply chain to prevent terrorists from shipping weapons of mass destruction (WMD) in one of the millions of cargo containers that arrive at U.S. ports each year. CBP has developed a layered security strategy to mitigate the risk of an attack using cargo containers. CBP's strategy is based on a layered approach of related programs that attempt to focus resources on potentially risky cargo shipped in containers while allowing other cargo containers to proceed without unduly disrupting commerce into the United States. The strategy is based on obtaining advanced cargo information to identify high-risk containers, utilizing technology to examine the content of containers, and partnerships with foreign governments and the trade industry. One of the programs in this layered security strategy is the Secure Freight Initiative (SFI). In December 2006, in response to SAFE Port Act requirements, DHS, and the Department of

Energy (DOE) jointly announced the formation of the SFI pilot program to test the feasibility of scanning 100 percent of U.S.-bound container cargo at three foreign ports (Puerto Cortes, Honduras; Qasim, Pakistan; and Southampton, United Kingdom). According to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement, CBP also selected the ports of Busan, South Korea; Hong Kong; Salalah, Oman; and Singapore to more fully demonstrate the capability of the integrated scanning system at larger, more complex ports. As of April 2010, SFI has been operational at five of these seven seaports.

In October 2009, we reported that CBP has made some progress in working with the SFI ports to scan U.S.-bound cargo containers; but because of challenges to expanding scanning operations, the feasibility of scanning 100 percent of U.S.-bound cargo containers at over 600 foreign seaports remains largely unproven.[24] CBP and DOE have been successful in integrating images of scanned containers onto a single computer screen that can be reviewed remotely from the United States. They have also been able to use these initial ports as a test bed for new applications of existing technology, such as mobile radiation scanners. However, the SFI ports' level of participation, in some cases, has been limited in terms of duration (e.g., the Port of Hong Kong participated in the program for approximately 16 months) or scope (e.g., the Port of Busan, Korea, allowed scanning in one of its eight terminals). In addition, the Port of Singapore withdrew its agreement to participate in the SFI program and, as of April 2010, the Port of Oman had not begun scanning operations. Furthermore, since the inception of the SFI program in October 2007, no participating port has been able to achieve 100 percent scanning. While 54 to 86 percent of the U.S.-bound cargo containers were scanned at three comparatively low-volume ports that are responsible for less than 3 percent of container shipments to the United States, sustained scanning rates above 5 percent have not been achieved at two comparatively larger ports—the type of ports that ship most containers to the United States. Scanning operations at the SFI ports have encountered a number of challenges—including safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images. Both we and CBP had previously identified many of these challenges, and CBP officials are concerned that they and the participating

[24]GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

ports cannot overcome them.[25] In October 2009, we recommended that DHS conduct a feasibility analysis of implementing the 100 percent scanning requirement in light of the challenges faced.[26] DHS concurred with our recommendation.

CBP and DOE spent approximately $100 million through June 2009 on implementing and operating the SFI program, but CBP has not developed a comprehensive estimate for future U.S. program costs, or conducted a cost-benefit analysis that compares the costs and benefits of the 100 percent scanning requirement with other alternatives. The SAFE Port Act requires CBP to report on costs for implementing the SFI program at foreign ports, but CBP has not yet estimated total U.S. program costs because of both the lack of a decision by DHS on a clear path forward and the unique set of challenges that each foreign port presents. While uncertainties exist regarding a path forward for the program, a credible cost estimate consistent with cost estimating best practices could better aid DHS and CBP in determining the most effective way forward for SFI and communicating the magnitude of the costs to Congress for use in annual appropriations. To address this, in October 2009, we recommended that CBP develop comprehensive and credible estimates of total U.S. program costs.[27] DHS concurred with our recommendation.

CBP and DOE have paid the majority of SFI costs for operating the SFI program. The SAFE Port and 9/11 Commission Acts do not address the issue of who is expected to pay the cost of developing, maintaining, and using the infrastructure, equipment, and people needed for the 100 percent scanning requirement, but implementing the requirement would entail costs beyond U.S. government program costs, including those incurred by foreign governments and private terminal operators, and could result in higher prices for American consumers. CBP has not estimated these additional economic costs, though they are relevant in assessing the balance between improving security and maintaining trade capacity and the flow of cargo. To address this, in October 2009, we recommended that DHS conduct a cost-benefit analysis to evaluate the costs and benefits of achieving 100 percent scanning as well as other alternatives for enhancing

[25]GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008).

[26] GAO-10-12.

[27]GAO-10-12.

container security.[28] Such an analysis could provide important information to CBP and to Congress to determine the most effective way forward to enhance container security. DHS agreed in part with our recommendation that it develop a cost-benefit analysis of 100 percent scanning, acknowledging that the recommended analyses would better inform Congress, but stated the recommendations should be directed to the Congressional Budget Office. While the Congressional Budget Office does prepare cost estimates for pending legislation, we think the recommendation is appropriately directed to CBP. Given its daily interaction with foreign customs services and its direct knowledge of port operations, CBP is in a better position to conduct any cost-benefit analysis and bring results to Congress for consideration.

Senior DHS and CBP officials acknowledge that most, if not all foreign ports, will not be able to meet the July 2012 target date for scanning all U.S.-bound cargo. Recognizing the challenges to meeting the legislative requirement, DHS expects to grant a blanket extension to all foreign ports pursuant to the statue, thus extending the target date for compliance with this requirement by 2 years, to July 2014. In addition, the Secretary of Homeland Security approved the "strategic trade corridor strategy," an initiative to scan 100 percent of U.S.-bound containers at selected foreign ports where CBP believes it will mitigate the greatest risk of WMD entering the United States. According to CBP, the data gathered from SFI operations will help to inform future deployments to strategic locations. CBP plans to evaluate the usefulness of these deployments and consider whether the continuation of scanning operations adds value in each of these locations, and potential additional locations that would strategically enhance CBP efforts. While the strategic trade corridor strategy may improve container security, it does not achieve the legislative requirement to scan 100 percent of U.S.-bound containers. According to CBP, it does not have a plan for full-scale implementation of the statutory requirement by July 2012 because challenges encountered thus far in implementing the SFI program indicate that implementation of 100 percent scanning worldwide by the 2012 deadline will be difficult to achieve. However, CBP has not performed a feasibility analysis of expanding 100 percent scanning, as required by the SAFE Port Act. To address this, in October 2009, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning and provide the results, as well as

[28] GAO-10-12.

alternatives to Congress, in order to determine the best path forward to strengthen container security.[29] DHS concurred with our recommendation.

In DHS's Congressional Budget Justification FY 2011, CBP requested to decrease the SFI program's $19.9 million budget by $16.6 million. According to the budget justification, in fiscal year 2011, SFI operations will be discontinued at three SFI ports—Puerto Cortes, Honduras; Southampton, United Kingdom; Busan, South Korea—and the SFI program will be established at the Port of Karachi, Pakistan. Furthermore, CBP's budget justification did not request any funds to implement the strategic trade corridor strategy.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the Committee may have at this time.

GAO Contacts 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. In addition to the contacts named above, John Mortin, Assistant Director, managed this review. Jonathan Bachman, Charles Bausell, Lisa Canini, Frances Cook, Tracey Cross, Andrew Curry, Anthony DeFrank, Geoff Hamilton, Dawn Hoff, Lara Miklozek, Stanley Kostyla, Jan Montgomery, and Kendal Robinson made key contributions to this statement.

[29] GAO-10-12.

Related GAO Products

Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps. GAO-10-883T. Washington, D.C.: June 30, 2010.

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. GAO-10-400. Washington, D.C.: April 9, 2010.

Coast Guard: Deployable Operations Group Achieving Organizational Benefits, but Challenges Remain. GAO-10-433R. Washington, D.C.: April 7, 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.

Coast Guard: Observations on the Requested Fiscal Year 2011 Budget, Past Performance, and Current Challenges. GAO-10-411T. Washington, D.C.: February 25, 2010.

Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers. GAO-10-12. Washington, D.C.: October 30, 2009.

Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation. GAO-09-492. Washington D.C.: March 27, 2009.

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed. GAO-09-337. Washington, D.C.: March 17, 2009.

Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-904T. Washington, D.C.: June 25, 2008.

Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers. GAO-08-533T. Washington, D.C., June 12, 2008.

Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-627SP. Washington, D.C.: April 15, 2008.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. GAO-08-141. Washington, D.C.: December 10, 2007.

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

Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Ports. GAO-08-86T. Washington, D.C.: October 4, 2007.

Information on Port Security in the Caribbean Basin. GAO-07-804R. Washington, D.C.: June 29, 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.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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