United States Government Accountability Office

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
10:30 a.m. ET
Wednesday, June 4, 2014

MARITIME SECURITY

Progress and Challenges with Selected Port Security Programs

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

June 4, 2014

MARITIME SECURITY

Progress and Challenges with Selected Port Security Programs

GAO Highlights

Highlights of GAO-14-636T, a testimony before the Senate Committee on Homeland Security and Governmental Affairs

Why GAO Did This Study

Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and their link to the global supply chain—that is, the flow of goods from manufacturers to retailers. Balancing security concerns with facilitation of the free flow of people and commerce remains an ongoing challenge for federal, state, local, and private stakeholders operating in ports.

Within DHS, several components are responsible for port security activities. These activities include, among other things, promoting maritime domain awareness, conducting port facility inspections, and screening incoming vessels' cargoes for the presence of contraband such as weapons of mass destruction, illicit drugs, or explosives.

This statement discusses progress and challenges in key areas of DHS port security programs. It is based on work GAO has previously conducted from September 2003 to September 2013 with selected updates conducted through May 2014. For these updates, GAO contacted DHS officials and reviewed relevant documents.

What GAO Recommends

In prior reports, GAO has made recommendations to DHS to strengthen various port security programs. DHS generally concurred with the recommendations and has taken actions, or has actions under way, to address most of these recommendations.

View GAO-14-636T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or CaldwellS@gao.gov

What GAO Found

GAO's prior work has shown that the Department of Homeland Security (DHS) and its component agencies—particularly the Coast Guard and Customs and Border Protection (CBP)—have made substantial progress in three key areas of port security since the September 11, 2001 terrorist attacks (9/11), but some challenges remain.

Maritime domain awareness and information sharing. DHS agencies along with other port partners have taken actions to enhance visibility over the maritime domain and facilitate cooperation among partners by collecting, assessing and sharing key information. However, some challenges remain in implementing the tools necessary to maintain this focus and increase coordination among stakeholders. For example, in multiple reports since 2011, GAO found the Coast Guard's weak management of technology acquisitions—that were focused on enhancing maritime awareness and increasing communication among partners—resulted in these acquisitions not fully achieving their intended purposes. DHS concurred with GAO's recommendations for addressing these weaknesses.

Security in domestic ports. Since 9/11, DHS components have taken a wide variety of actions to better secure domestic ports. For example, the Coast Guard has assessed risks to cruise ships in accordance with DHS guidance and is providing escorts for high-risk vessels such as cruise ships and ferries while CBP is reviewing passenger and crew data to target inspections. In addition, since 2002, the Federal Emergency Management Agency (FEMA) has provided almost $2.9 billion in federal funding through the Port Security Grant Program (PSGP) to help defray the cost of implementing security efforts in many ports and has established measures to improve the administration of the PSGP. However, in 2014 FEMA stated that it is unable—due to resource constraints—to annually measure reduced vulnerability attributed to enhanced PSGP-funded security measures. Meanwhile, the Transportation Security Administration (TSA) and the Coast Guard have been administering a program requiring maritime workers to obtain a biometric identification card to gain access to certain facilities. However, in 2011, GAO recommended that DHS assess internal controls to identify actions needed to address, among other things, weaknesses governing enrollment and background checks. As of March 2014 this action had not been completed.

Protection of the global supply chain. DHS agencies, especially CBP, have taken steps to enhance the security of the global supply chain—particularly for cargo bound for the United States. Efforts have focused on assessing and mitigating cargo risk before it enters U.S. ports by better targeting and scanning cargo, and establishing security partnerships with the foreign countries and companies that ship cargo to the United States. However, in multiple reports since 2005, GAO found that DHS programs focused on protecting the global supply chain have been implemented with varying degrees of success and that many would benefit from the DHS agencies conducting further assessments of the programs, among other things. GAO has made recommendations to address these issues and DHS has concurred or generally concurred with most of these recommendations and has taken actions to address many of them.

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to discuss the Department of Homeland Security's (DHS) ongoing port security efforts and programs. Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and the ready access the ports have to transportation links into the United States. An attack on a large port could also have a widespread impact on the broader global supply chain—the flow of goods from manufacturers to retailers—and the world economy. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for federal, state, local, and private stakeholders operating in ports.

Within DHS, several components, including the Office of Policy, the U.S. Coast Guard, U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the Domestic Nuclear Detection Office (DNDO), and the Federal Emergency Management Agency (FEMA) are responsible for port security activities. These activities include, among other things, promoting maritime domain awareness, conducting port facility and commercial vessel inspections, and screening incoming vessels' cargoes for the presence of contraband such as weapons of mass destruction (WMD), illicit drugs, or explosives, while facilitating the flow of legitimate trade and passengers.

My statement today discusses progress and challenges with DHS programs responsible for enhancing port security. Specifically, I will address maritime domain awareness and information sharing, security in domestic ports, and protection of the global supply chain.

My statement is based on reports and testimonies we issued from September 2003 through September 2013 related to maritime, port, vessel, and cargo security—with selected updates on how DHS responded to our prior recommendations, which we conducted through May 2014. 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. For the selected updates, we contacted DHS officials and reviewed relevant documents pertaining to the status of recommendation implementation. Further details on the scope and methodology for the previously issued reports and testimonies are available within each of the published products. A list of products on which this statement is based is included at the end of the statement. 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.

Background

Legislation, Strategies, and Plans

Since the terrorist attacks of September 11, 2001 (9/11), Congress established a new port security framework—much of which was set in place by the Maritime Transportation Security Act of 2002 (MTSA) and the Security and Accountability For Every Port Act of 2006 (SAFE Port Act).[1] This framework is implemented through various strategies and plans, and the combined efforts of several DHS components.

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 major requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for ports, port facilities, and vessels; (3) developing a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing a process to assess the security levels of foreign ports from which vessels depart on voyages to the United States.

In 2006, the SAFE Port Act, which in part amended MTSA, became law. The SAFE Port Act required DHS to develop, implement, and update, as appropriate, a strategic plan to enhance the security of the international supply chain—the flow of goods from manufacturers to retailers. Further,

[1]Pub. L. No. 107-295, 116 Stat. 2064; Pub. L. No. 109-347, 120 Stat. 1884.

the SAFE Port Act required DHS to establish pilot projects at three ports to test the feasibility of scanning 100 percent of U.S.-bound cargo containers at foreign ports.

The federal government has made progress in national and port-level security planning by developing strategies and plans. Specifically, the National Strategy for Maritime Security, published in September 2005, aimed to align all federal government maritime security programs and activities into a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities.[2] Further, the Coast Guard has developed Area Maritime Security Plans (AMSP) to enhance the security of domestic ports around the country. Applicable governmental and private entities contribute to the AMSPs, which serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response.

Roles and Responsibilities

DHS is the lead federal department and with its component agencies has responsibility for administering much of the port security framework, DHS and its components must balance security priorities with the need to facilitate legitimate trade through the efforts of several component agencies. DHS components with port security responsibilities include:

- **Office of Policy**: The Office of Policy leads the coordination, integration, and development of DHS-wide policies, programs, strategies, and plans.
- **U.S. Coast Guard**: The Coast Guard, among other things, conducts port facility and commercial vessel inspections and leads the coordination of maritime information-sharing efforts.
- **TSA**: TSA has lead 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.

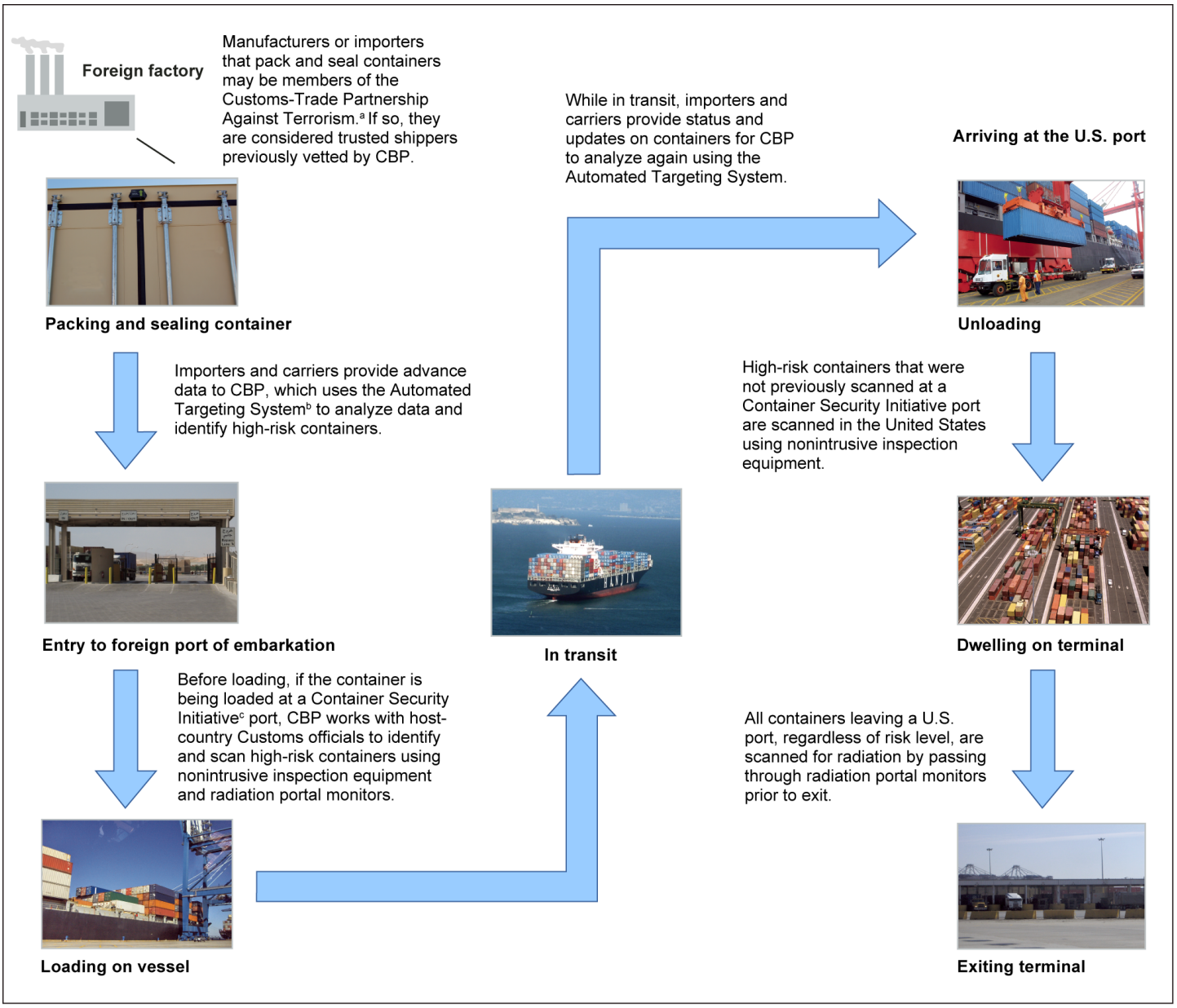
[2]Homeland Security Presidential Directive 13 (HSPD-13) directed the Secretaries of Defense and Homeland Security to lead a joint effort to draft the national strategy. HSPD-13 also directed DHS to develop eight supporting implementation plans to address the specific threats and challenges of the maritime environment. These plans include overarching strategies such as the *National Plan to Achieve Maritime Domain Awareness* and are implemented by specific plans such as the *Countering Piracy off the Horn of Africa: Partnership & Action Plan*.

- **DNDO**: DNDO 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.

- **FEMA:** FEMA is responsible for administering grants to improve the security of the nation's highest-risk port areas.

- **CBP**: CBP is responsible for the screening of incoming vessels' crew and cargoes for the presence of contraband, such as WMDs, illicit drugs, or explosives. As shown in figure 1, CBP programs are involved throughout the global supply chain process.

Figure 1: Global-Supply Chain Process



Source: GAO (analysis); GAO and DHS S&T (photos); Art Explosion (clipart). | GAO-14-636T

[a]The Customs-Trade Partnership Against Terrorism is a voluntary program designed to improve the security of the international supply chain while maintaining an efficient flow of goods. Under this program, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security.

[b]The Automated Targeting System is a mathematical model that uses weighted rules to assign a risk score to arriving cargo shipments based on shipping information. CBP uses the Automated Targeting System as a decision support tool in targeting cargo containers for inspection.

[c] The Container Security Initiative places CBP staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for WMDs before it is shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that the officials' foreign counterparts examine the contents of the containers.

DHS Has Made Substantial Progress in Enhancing Port Security, but Challenges Remain

Our prior work has shown that DHS and its component agencies—particularly the Coast Guard and CBP—have made substantial progress in implementing various programs that, collectively, have enhanced port security but some challenges remain. Examples of progress and challenges in the areas of (1) enhancing maritime domain awareness and information sharing, (2) increasing security in domestic ports, and (3) protecting the global supply chain are discussed below.

Maritime Domain Awareness and Information Sharing

DHS, its component agencies, and other port partners have taken a variety of actions to enhance visibility of the maritime domain and facilitate cooperation among partners by collecting, assessing and sharing key maritime domain information, but challenges remain. Timely awareness of the maritime domain, and knowledge of threats helps the Coast Guard and other agencies to detect, deter, interdict, and defeat adversaries.

- **Interagency operations centers**: Interagency operations centers (IOCs) are physical or virtual centers of collaboration to improve maritime domain awareness and operational coordination among port partners—including federal, state, and local law enforcement agencies. Port partners are able to use these centers to participate in maritime security activities, such as the implementation and administration of intelligence activities, information sharing, and vessel tracking. The SAFE Port Act required the establishment of certain IOCs, and the Coast Guard Authorization Act of 2010 further specified that IOCs must provide, where practicable, for the physical colocation of the Coast Guard with its port partners, and that IOCs must include information management systems.[3] In February 2012, we reported that the Coast Guard is continuing its efforts to establish IOCs at 35 locations and share maritime domain awareness information with its port partners.[4] However, we identified

[3]46 U.S.C. § 70107a.

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

factors that jeopardized the centers from meeting their purpose of improving information sharing and enhancing maritime domain awareness across federal, state, and local port partners, including weak management of the Interagency Operations Center Acquisition Project which was to provide information-management tools to improve interagency coordination, enhance awareness, and automate anomaly detection. As a result, we made five recommendations to address these issues—including recommendations related to improving the Coast Guard's process for collecting data and incorporating port partners' input into the development of requirements for an information-management and sharing system that would facilitate the IOCs. The Coast Guard concurred with these recommendations but has not implemented them, stating that neither the President's fiscal year 2013 nor fiscal year 2014 budget requested resources for the Interagency Operations Center Acquisition Project.

- **Common Operating Picture**: In general, the Coast Guard's Common Operating Picture (COP) can be described as a map-based information system— that can be shared among Coast Guard commands—that displays vessels, information about those vessels and the environment surrounding them. As a way to display COP information, the Coast Guard in 2010 deployed the Enterprise Geographic Information System (EGIS).[5] However as we reported in April 2013, there have been numerous issues with EGIS.[6] For example, Coast Guard information technology (IT) officials told us they had experienced challenges in meeting its goals for the system largely related to insufficient computational power on some Coast Guard workstations, a lack of training for users and system installers, and inadequate testing of EGIS software before installation. Consequently, the Coast Guard began developing a new COP-related technology, Coast Guard One View (CG1V). However, as we also reported in our April 2013 report, the Coast Guard did not follow its own IT development guidance when implementing CG1V. As a result, we recommended that the Coast Guard issue guidance clarifying the application of the System Development Life Cycle (SDLC) for the development of future projects. The Coast Guard concurred with the

[5] EGIS is the Coast Guard's geographic information system used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes.

[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).

recommendation and reported that it planned to issue guidance and clarify procedures regarding the applicability of the SDLC. In January 2014, the Coast Guard updated its SDLC tailoring plan. We reviewed the updated plan and determined that while it represented progress, it did not fully meet the intent of our recommendation because it was focused narrowly on the COP acquisition rather than more broadly clarifying procedures regarding the applicability of the SDLC for other IT projects as well. As a result, this recommendation remains open.

- **Vessel and aircraft maritime domain awareness**: To further enhance its ability to monitor the maritime domain, the Coast Guard planned to build a command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) system and put this system on all of its planes and larger vessels.[7] This system was designed to improve the probability of executing a successful mission by increasing the speed and accuracy of the Coast Guard's process of surveying the maritime domain, detecting and classifying targets, and then responding to the situation. A planned system-of-systems concept was intended to connect Coast Guard assets through a single command and control architecture—C4ISR.[8] However, in July 2011, we reported that the Coast Guard had not met its goal of building the $2.5 billion C4ISR system.[9] Specifically, we reported that the Coast Guard had repeatedly changed its strategy for achieving the C4ISR system's goal of building a single fully interoperable command, control, intelligence, surveillance, and reconnaissance system across the Coast Guard's new vessels and aircraft. Further, we found that not all aircraft and vessels were operating the same C4ISR system, or even at the same classification level, and hence could not directly exchange data with one another. Given these uncertainties, we concluded that the Coast Guard did not have a clear vision of the C4ISR required to meet its missions. In response to our recommendation, the Coast Guard has developed needed documentation and truncated portions of the program. The Coast Guard is now working toward the goal of developing compatible and

[7]In July 2011, we reported that the Coast Guard was developing C4ISR infrastructure that it expected to collect, correlate, and present information into a single COP to facilitate mission execution. See GAO, *Coast Guard: Action Needed as Approved Deepwater Program Remains Unachievable*, GAO-11-743 (Washington, D.C.: July 28, 2011).

[8]A system-of-systems is a set or arrangement of assets that results when independent assets are integrated into a larger system that delivers unique capabilities.

[9]GAO-11-743.

manageable software packages on major cutters and medium-and long-range planes. We will continue to assess the C4ISR program through our ongoing work on Coast Guard recapitalization efforts and expect to issue a report in summer 2014.

Security in Domestic Ports

Port stakeholders and DHS component agencies have implemented a wide variety of security measures that are intended to better secure U.S. ports. For example, in 2003, the Coast Guard issued regulations requiring offshore facility and port and operators to enhance their own security through the implementation of security plans for their facilities.[10] Further, the Port Security Grant Program was established in 2002, and through FEMA's management of this program, federal grant funding is made available to states, localities and private parties to help defray the costs of required security measures. Other security measures directly involving DHS agencies include Coast Guard inspections and escorts of high-risk vessels, among other actions.

- **Port and offshore facility security plans and inspections**: To enhance the security of port facilities, the Coast Guard has implemented regulations and programs requiring port facility security plans. Owners and operators of certain maritime facilities are required to conduct assessments of security vulnerabilities, develop security plans to mitigate these vulnerabilities. The Coast Guard inspects these facilities annually. In addition to inspecting port facilities, the Coast Guard also conducts inspections of offshore facilities, such as oil rigs. In our October 2011 report on inspections of offshore energy facilities, we found that the Coast Guard had taken actions to help ensure the security of offshore energy facilities, such as developing and reviewing security plans, but faced difficulties ensuring that all facilities complied with requirements.[11] We recommended that the Coast Guard develop policies and procedures to ensure that annual security inspections are conducted and information entered into databases is more useful for management. The Coast Guard concurred with these recommendations and is in the process of updating its guidance for Coast Guard units and program managers. In February 2014, Coast Guard officials told us that the Coast Guard plans to improve its inspection database by March 2015.

[10] 33 C.F.R. §§ 105.400-.415, 106.400-.415.

[11] GAO, *Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure,* GAO-12-37 (Washington, D.C.: Oct. 28, 2011).

- **Port Security Grant Program**: To help defray some of the costs of implementing security at ports around the United States, the Port Security Grant Program was established in January 2002 and since then has awarded almost $2.9 billion for port security efforts.[12] The Port Security Grant Program awards funds to states, localities, and private port stakeholders to strengthen the nation's ports against risks associated with potential terrorist attacks. We reported in November 2011 that, for fiscal years 2010 and 2011, allocations of these funds were based on DHS's risk model and implementation decisions were made largely in accordance with risk.[13] For example, we found that allocations of funds to port areas were highly positively correlated to port risk, as calculated by DHS's risk model. However, we also noted that the method used to calculate vulnerability—a port's relative exposure to an attack—could be strengthened to better account for how the implementation of grant-funded security projects affects a port's vulnerability score. Accordingly, we recommended that DHS develop a vulnerability index that accounts for how security improvements affect port vulnerability, and incorporate these changes into future iterations of the grant's risk model. In February 2014, FEMA officials stated that they have determined that this specific enhancement is not achievable, in part because the agency lacks the resources to annually measure the reduced vulnerability attributed to enhanced PSGP security measures. However, they also stated that FEMA remains committed to improving the measure of vulnerability within the grant's risk model. In our 2011 report, we also raised questions about the effectiveness of the administrative management of the grant program, and we recommended that FEMA develop timeframes and related milestones for implementing performance measures. In February 2014, FEMA officials provided documentation of management and administrative performance measures to help strengthen the implementation, administration and oversight of the PSGP, and thus we have closed this recommendation.

- **Personnel access to port facilities**: The Transportation Worker Identification Credential (TWIC) program, administered by TSA and the Coast Guard, requires maritime workers to undergo background checks and obtain a biometric identification card to gain unescorted access to

[12]Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002). MTSA codified the program when it was enacted in November 2002. 46 U.S.C. § 70107.

[13]GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened,* GAO-12-47 (Washington, D.C.: Nov. 17, 2011).

secure areas of regulated maritime facilities. Initiated in December 2001, we have been reporting on TWIC progress and challenges since September 2003.[14] Among other issues, we have highlighted steps that TSA and the Coast Guard have taken to meet an expected surge in initial enrollment as well as various challenges experienced in the TWIC testing conducted by a contractor for TSA and the Coast Guard from August 2004 through June 2005. We also identified challenges related to ensuring that the TWIC technology works effectively in the harsh maritime environment.[15]

In November 2009, we reported on the design and approach of a pilot initiated in August 2008 to test TWIC readers, and found that DHS did not have a sound evaluation methodology to ensure information collected through the TWIC reader pilot would be complete and accurate.[16] As a result, we recommended that the DHS components implementing the pilot—TSA and Coast Guard—develop an evaluation plan to guide the remainder of the pilot and identify how they will compensate for areas where the TWIC reader pilot would not provide the information. DHS agreed and took initial steps, but did not develop an evaluation plan, as we recommended. Moreover, in May 2011, we reported that internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals.[17] Accordingly, in our 2011 report, we recommended that DHS assess TWIC program internal controls to identify needed corrective actions, assess TWIC's effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. While DHS concurred with our recommendation, as

[14]GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

[15]GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006). TWIC readers and related technologies operated outdoors in the harsh maritime environment can be affected by dirt, salt, wind, and rain.

[16]GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

[17]GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

of May 2013 DHS had not taken significant action to address our recommendation. We therefore reaffirmed this recommendation in May 2013, recommending to Congress that it repeal a requirement that DHS issue regulations consistent with the TWIC reader pilot and instead require DHS to complete an assessment that evaluates the effectiveness of using TWIC with readers for enhancing port security, and then use the results of the assessment to promulgate a final regulation as appropriate.[18]

In January 2014, the explanatory statement accompanying the Consolidated Appropriations Act, 2014, directed DHS to complete the TWIC program assessment that we recommended within 90 days after the enactment of the Consolidated Appropriations Act of 2014 (by April 17, 2014).[19] As of March 2014, DHS had taken steps toward addressing our 2011 recommendation, such as developing a list of control issues we identified in 2011 and establishing an Executive Steering Committee to address the recommendations. However, TSA had no estimate for when the effectiveness assessment would be completed.

- **Operations and escorts**: To further protect ports, DHS agencies assess risks, conduct inspections, and escort high-risk vessels. For example, the Coast Guard has assessed risks to cruise ships in accordance with DHS guidance—which requires that the agency analyze threats, vulnerabilities, and consequences. CBP reviews passenger and crew data to help target inspections. In addition, the Coast Guard escorts a certain percentage of high-capacity passenger vessels—cruise ships, ferries, and excursion vessels—to protect against external threats, such as a waterborne improvised explosive device. Specifically, the Coast Guard has provided escorts for cruise ships to help prevent waterside attacks and has provided a security presence on passenger ferries during their transits. Further, the Coast Guard has conducted energy commodity tanker security activities, such as security boardings, escorts, and

[18]GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198 (Washington, D.C.: May 8, 2013).

[19]Explanatory statement accompanying Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5.

patrols. Such actions enhance the security of these vessels, thereby also protecting the ports in which they operate.[20]

Protection of the Global Supply Chain

DHS agencies have also taken steps to enhance the security of cargo bound for the United States—even before it arrives in U.S. ports. Some of these efforts have focused on increasing the volume, accuracy and timing of information available to DHS agencies for assessing cargo risk. Other efforts have involved an increased use of technology such as scanners. DHS agencies have also taken steps to enhance U.S. port security by establishing security measures and partnerships with the foreign countries and companies that ship cargo to the United States—so that cargo risk is assessed and mitigated before the cargo may enter U.S. ports. These various measures and programs have been implemented with varying degrees of success.

- **Cargo screening and the Automated Targeting System**: As part of its efforts to target high-risk maritime cargo containers for inspection, CBP screens containers in advance of their arrival in the United States. To enhance the screening of these containers, DHS developed the Automated Targeting System (ATS)–a computerized system that assesses information on each U.S.-bound cargo shipment and assigns it a risk score. CBP officers then use this risk score, along with other information, such as the shipment's contents, to determine which shipments to physically examine. In September 2010, we reported that CBP had made progress in implementing ATS and enhancing it through the use of additional data.[21] However, in 2012, we also found that more regular assessments of ATS were needed to enhance its targeting of maritime cargo containers and better position CBP to provide reasonable assurance of the effectiveness of ATS. We therefore recommended that the Commissioner of CBP (1) ensure that future updates to the rules that

[20]For additional information on the Coast Guard's role in protecting and/or escorting certain vessels, please see the following GAO reports. GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010); *Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security,* GAO-11-207 (Washington, D.C.: Dec. 3, 2010); *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.: Dec. 10, 2007).

[21]GAO, *Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain*, GAO-10-841 (Washington, D.C.: Sept. 10, 2010).

identify risks are based on results of assessments that demonstrate the effectiveness of such updates; and (2) establish targets for CBP's performance measures and use those measures to assess the effectiveness of ATS on a regular basis to better determine when updates to the rules that identify risks are needed.[22] CBP concurred with the recommendations and in May 2014 provided milestones for implementing the recommendations by June 2015.

- **Deploying scanning technologies**: Once cargoes such as those shipped in containers arrive in U.S. ports, DHS deploys various technologies to scan their contents. DHS technological improvements have been focused on developing and deploying equipment to scan cargo containers for nuclear materials and other contraband to better secure the supply chain. Specifically, to detect nuclear materials, CBP, in coordination with DNDO, has deployed over 1,400 radiation portal monitors at U.S. ports of entry. Most of the radiation portal monitors are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass. These monitors trigger an alarm when they detect radiation coming from a vehicle or shipping container. CBP then conducts further inspections at its secondary inspection locations to identify the cause of the alarm and determine whether there is a reason for concern. In 2005, DNDO began working with CBP on a program to develop and test a type of next-generation radiation portal monitor—the advanced spectroscopic portal (ASP)—designed to both detect radiation and identify the source as benign, suspect, or a threat.[23] The initial concept of the program was to develop, procure, and deploy enough ASPs to replace many of CBP's currently deployed radiation portal monitors and handheld detectors at a cost of $2 billion to $3 billion, according to DNDO. However, in 2007, we found that the initial testing related to DNDO's efforts to develop and procure the ASP was not

[22]GAO, *Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System*, GAO-13-9 (Washington, D.C.: Oct. 25, 2012).

[23]GAO, *Combating Nuclear Smuggling: Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisitions,* GAO-13-256 (Washington, D.C.: May 13, 2013). As we reported in 2013, ASP may have reduced the rate of alarms that are triggered by benign radioactive materials that naturally occur in common items such as kitty litter and granite. The reduced rate of alarms may also have reduced the number of unnecessary secondary screenings.

rigorous enough.[24] Once the testing became more rigorous, these portals did not perform well enough to warrant deployment. Accordingly, DHS scaled back the program in 2010 and subsequently canceled the program in 2012, after DNDO had spent more than $280 million on development and testing.

- **CSI program overseas**: CBP has also developed the Container Security Initiative (CSI) program, which places CBP officials at selected foreign ports to use intelligence and risk assessment information to work with host country officials to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing WMDs or other terrorist contraband.[25] 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. In September 2013, we reported that CBP had not assessed the risk posed by foreign ports that ship cargo to the United States since 2005 and recommended that DHS direct CBP to periodically assess the risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to inform any future adjustments to CSI locations.[26] DHS concurred and reported that, by December 2014, it plans to develop a process for conducting such periodic risk assessments. In addition, in a May 2014 letter to Congress, the Secretary of Homeland Security reported that DHS will work to increase the percentage of containers scanned abroad and will engage other countries to discuss the potential expansion of CSI to additional ports that ship high-risk cargo to the United States.

- **Megaports Initiative**: We reported in 2005 and 2012 on the Megaports Initiative—a National Nuclear Security Administration (NNSA) nonproliferation program that funds the installation of radiation detection

[24]For further information regarding our work on the advanced spectroscopic portal, see GAO, *Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment*, GAO-07-1247T (Washington, D.C.: Sept. 18, 2007); and *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology,* GAO-09-655 (Washington, D.C.: May 29, 2009).

[25]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.

[26]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).

equipment at seaports overseas.[27] The Initiative seeks to deter, detect, and interdict nuclear or other radiological materials from being smuggled through foreign seaports. At the time of our 2012 report, NNSA had completed 42 of 100 planned Megaports in 31 countries. NNSA equipped these seaports with radiation detection equipment and established training programs for foreign personnel. However, in 2012, we found that the Megaports Initiative and DHS's Container Security Initiative were not sufficiently coordinated. For example, in two countries where both programs were operating, DHS officials told us that they were using personal radiation detectors—a type of equipment intended for personal safety but not appropriate for scanning containers—to inspect containers if their radiation detection equipment was broken. In both countries, the Megaports Initiative had more suitable equipment that DHS officials could have used to improve detection capabilities. We made several recommendations in our 2012 report, including that NNSA and DHS jointly assess the extent to which the two initiatives are effectively coordinated. In response to this recommendation, in December 2012, NNSA established standard operating procedures that formalized coordination between the two programs. Subsequently, the administration concluded that there were diminishing returns for new Megaports and limitations in the effectiveness of the technologies used and proposed reducing the initiative's fiscal year 2013 budget by about 85 percent. As a result, NNSA had planned to shift the initiative's focus from establishing new Megaports to sustaining existing ones. However, we reported in 2012 that NNSA had not finalized a long-term plan for ensuring the sustainability of Megaports operations and recommended that NNSA finalize this plan. In response to this recommendation, in October 2012, NNSA finalized its sustainability plan.

- **Secure Freight Initiative**: The Secure Freight Initiative (SFI) established pilot projects to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports to address concerns that terrorists would smuggle WMDs inside cargo containers bound for the United States. We testified in June 2008 that CBP faced difficulties in implementing SFI because of challenges related to host nation examination practices, performance measures, resource constraints, logistics, and technology

[27]See GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005) and *Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges*, GAO-13-37 (Washington, D.C.: Oct. 31, 2012).

limitations.[28] In October 2009, we issued a report on SFI and recommended, among other things, that DHS, in consultation with the Secretaries of Energy and State, conduct cost-benefit and feasibility analyses and provide the results to Congress. CBP partially concurred with these recommendations, but CBP officials told us that CBP does not plan to conduct the analyses because it has insufficient funds to conduct such analyses. The SAFE Port Act, as amended in 2007 by the Implementing Recommendations of the 9/11 Commission Act, directed DHS to implement 100 percent scanning of U.S.-bound maritime cargo container shipments by July 2012, but authorized DHS to extend the deadline for 2 years and renew such extension in additional 2-year increments if at least two of six statutory conditions existed.[29] The former DHS Secretary exercised this authority and formally notified Congress by letter dated May 2, 2012 that she had extended the deadline until July 1, 2014. In a letter to Members of Congress, in May 2014, the Secretary of Homeland Security stated that the conditions and supporting evidence cited in the 2012 deadline extension—negative effects on trade capacity and the flow of cargo and characteristics of foreign ports that prevent the installation of scanning systems— continue to prevail and preclude full-scale implementation.

- **Partnerships with industry**: 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. Companies that join the C-TPAT program commit to improving the security of their supply chains and 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. In return for their participation in the program, C-TPAT members are entitled to a reduced likelihood of scrutiny of their cargo. In April 2008, we found that the C-TPAT program held promise as part of CBP's multifaceted maritime security strategy.[30] We also found that the program allows CBP

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

[29] Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)).

[30]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).

to develop partnerships with the international trade community and provides CBP with a level of information sharing that would otherwise not be available due to CBP's usual jurisdiction and activities. However, our report raised questions about the management of the program's records and performance, and challenges in verifying that C-TPAT members meet security criteria. Thus, we recommended in 2008 that CBP strengthen program management by developing planning documents and performance measures, and by improving the process for validating security practices of C-TPAT members. CBP agreed with these recommendations and, in 2009, completed its development of policies, performance measures and guidance to ensure process improvements.

- **International Port Security program**: 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 both foreign and U.S. ports, and the vessels arriving in U.S. ports. 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 visited over 100 countries and found that most had substantially implemented international standards.[31] In September 2012, we reported that the Coast Guard had made progress with implementing its International Port Security program despite a number of challenges.[32] For example, we reported that the Coast Guard was able to alleviate sovereignty concerns of some countries by inviting foreign delegations to visit U.S. ports. Further, as we reported in September 2013, the Coast Guard had visited port facilities in over 150 countries by June of 2013 and developed a risk-informed model—that it updates annually—as part of its International Port Security program.[33] The Coast Guard uses the model to make informed decisions on how to engage each country within 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 to enhance its port security.

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

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

[33]GAO-13-764.

- **Mutual recognition**: 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.[34] 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.[35] In September 2013, we found that mutual recognition arrangements may allow the Coast Guard to allocate resources more efficiently and reduce risks.[36] For example, we 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.[37] 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 arrangements increases efficiencies and noted that they intend to negotiate additional

[34]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.

[35]The World Customs Organization is an intergovernmental organization representing the customs administrations of 179 countries, which aims to enhance the effectiveness and efficiency of Customs administrations.

[36]GAO-13-764.

[37]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.

memorandums of understanding with other foreign governments that have strong port inspection programs.

Thank you Chairman Carper, Ranking Member Coburn, and Members of the Committee. This completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For information 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. Other individuals making key contributions included Dawn Hoff, Assistant Director, Laurier Fish, Kevin Heinz, Tyler Kent, Amanda Kolling, Glen Levis, Kevin Tarmann, Katherine Trimble, and Edwin Woodward. Additional contributors include Jonathan Bachman, Christopher Conrad, Frances Cook, Katherine Davis, Michele Fejfar, Alana Finley, Paul Hobart, Katherine Lee, and Tracey King.

Related GAO Products

Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports. GAO-13-764. Washington, D.C.: September 16, 2013.

Combating Nuclear Smuggling: Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisition. GAO-13-256. Washington, D.C.: May 13, 2013.

Transportation Worker Identification Credential: Card Reader Pilot Are Unreliable; Security Benefits Need to Be Reassessed. GAO-13-198. Washington, D.C.: May 8, 2013.

Coast Guard: Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program. GAO-13-321. Washington, D.C.: April 25, 2013.

Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges. GAO-13-37. Washington, D.C.: October 31, 2012.

Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System, GAO-13-9. October 25, 2012.

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

Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers. GAO-12-202. Washington, D.C.: February 13, 2012.

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

Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure. GAO-12-37. Washington, D.C.: October 28, 2011.

Coast Guard: Action Needed as Approved Deepwater Program Remains Unachievable. GAO-11-743. Washington, D.C.: July 28, 2011.

Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives. GAO-11-657. Washington, D.C.: May 10, 2011.

Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security. GAO-11-207. Washington, D.C.: December 3, 2010.

Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain. GAO-10-841. Washington, D.C.: September 10, 2010.

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

Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers. GAO-10-43. Washington, D.C.: November 18, 2009.

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.

Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology. GAO-09-655. Washington, D.C.: May 29, 2009.

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

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.: April 25, 2008.

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.: February 14, 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.

Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment. GAO-07-1247T. Washington, D.C.: September 18, 2007.

Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program. GAO-06-982. Washington, D.C.: September 29, 2006.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO-05-375. Washington, D.C.: March 31, 2005.

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T. Washington, D.C.: September 9, 2003.