

**\*\*\*Excerpts on Maritime Security\*\*\***

September 2011

DEPARTMENT OF  
HOMELAND  
SECURITY

Progress Made and  
Work Remaining in  
Implementing  
Homeland Security  
Missions 10 Years  
after 9/11

\*\*\* Includes cover page, highlights, and section  
on maritime security (pp. 103-115)\*\*\*

U.S. Government Accountability Office

GAO 90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

## Why GAO Did This Study

The events of September 11, 2001, led to profound changes in government policies and structures to confront homeland security threats. Most notably, the Department of Homeland Security (DHS) began operations in 2003 with key missions that included preventing terrorist attacks from occurring in the United States, and minimizing the damages from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than \$50 billion. Since 2003, GAO has issued over 1,000 products on DHS's operations in such areas as border and transportation security and emergency management, among others. As requested, this report addresses DHS's progress in implementing its homeland security missions since it began operations, work remaining, and issues affecting implementation efforts. This report is based on GAO's past and ongoing work, supplemented with DHS Office of Inspector General reports, with an emphasis on reports issued since 2008. GAO also analyzed information provided by DHS in July and August 2011 on recent actions taken in response to prior work.

## What GAO Recommends

While this report contains no new recommendations, GAO previously made about 1,500 recommendations to DHS. The department addressed about half of them, has efforts under way to address others, and has taken additional action to strengthen its operations. In commenting on this report, DHS stated that the report did not address all of DHS's activities. This report is based on prior work, which GAO reflects throughout the report.

View [GAO-11-881](#) or key components. For more information, contact Cathleen A. Berrick at (202) 512-3404 or [berrickc@gao.gov](mailto:berrickc@gao.gov).

## DEPARTMENT OF HOMELAND SECURITY

# Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

## What GAO Found

Since it began operations in 2003, DHS has implemented key homeland security operations and achieved important goals and milestones in many areas to create and strengthen a foundation to reach its potential. As it continues to mature, however, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. DHS's accomplishments include developing strategic and operational plans; deploying workforces; and establishing new, or expanding existing, offices and programs. For example, DHS

- issued plans to guide its efforts, such as the Quadrennial Homeland Security Review, which provides a framework for homeland security, and the *National Response Framework*, which outlines disaster response guiding principles;
- successfully hired, trained, and deployed workforces, such as a federal screening workforce to assume security screening responsibilities at airports nationwide; and
- created new programs and offices to implement its homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to help coordinate efforts to address cybersecurity threats.

Such accomplishments are noteworthy given that DHS has had to work to transform itself into a fully functioning department while implementing its missions—a difficult undertaking that can take years to achieve. While DHS has made progress, its transformation remains high risk due to its management challenges. Examples of progress made and work remaining include:

**Border security.** DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology program to verify the identities of foreign visitors entering and exiting the country by processing biometric and biographic information. However, DHS has not yet determined how to implement a biometric exit capability and has taken action to address a small portion of the estimated overstay population in the United States (individuals who legally entered the country but then overstayed their authorized periods of admission). DHS also deployed infrastructure to secure the border between ports of entry, including more than 600 miles of fencing. However, DHS experienced schedule delays and performance problems with the Secure Border Initiative Network, which led to the cancellation of this information technology program.

**Aviation security.** DHS developed and implemented Secure Flight, a program for screening airline passengers against terrorist watchlist records. DHS also developed new programs and technologies to screen passengers, checked baggage, and air cargo. However, DHS does not yet have a plan for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements, a mechanism to verify the accuracy of data to help ensure that air cargo screening is being conducted at reported levels, or approved technology to screen cargo once it is loaded onto a pallet or container.

**Emergency preparedness and response.** DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-

based preparedness, and a Target Capabilities List to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS is also finalizing a National Disaster Recovery Framework, and awards preparedness grants based on a reasonable risk methodology. However, DHS needs to strengthen its efforts to assess capabilities for all-hazards preparedness, and develop a long-term recovery structure to better align timing and involvement with state and local governments' capacity. DHS should also improve the efficacy of the grant application process by mitigating duplication or redundancy within the various preparedness grant programs.

**Chemical, biological, radiological and nuclear (CBRN) threats.** DHS assessed risks posed by CBRN threats and deployed capabilities to detect CBRN threats. However, DHS should work to improve its coordination of CBRN risk assessments, and identify monitoring mechanisms for determining progress made in implementing the global nuclear detection strategy.

GAO's work identified three themes at the foundation of DHS's challenges.

**Leading and coordinating the homeland security enterprise.** DHS has made important strides in providing leadership and coordinating efforts among its stakeholders. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In 2005, GAO designated information sharing for homeland security as high risk because the federal government faced challenges in analyzing and sharing information in a timely, accurate, and useful way.

**Implementing and integrating management functions for results.** DHS has enhanced its management functions, and has plans in place to further strengthen the management of the department for results. However, DHS has not always effectively executed or integrated these functions. In 2003, GAO designated the transformation of DHS as high risk because DHS had to transform 22 agencies into one department. DHS has demonstrated strong leadership commitment and begun to implement a strategy to address its management challenges. However, these challenges have contributed to schedule delays, cost increases, and performance problems in a number of programs aimed at delivering important mission capabilities, such as a system to detect certain nuclear materials in vehicles and containers at ports. DHS also faced difficulties in deploying some technologies that meet defined requirements. Further, DHS does not yet have enough skilled personnel in various areas, such as acquisition management; and has not yet developed an integrated financial management system, impacting its ability to have ready access to reliable information for informed decision making.

**Strategically managing risks and assessing homeland security efforts.** Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats have impacted DHS's approaches and investments. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs in an efficient manner.

Given DHS's leadership responsibilities in homeland security, it is critical that its programs are operating as efficiently and effectively as possible, are sustainable, and continue to mature to address pressing security needs. Eight years after its creation and 10 years after September 11, 2001, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

---

# Appendix VIII: Maritime Security

---

## What This Area Includes



Source: U.S. Coast Guard.  
Port of Los Angeles.

Within the Department of Homeland Security (DHS), the U.S. Coast Guard has primary responsibility for maritime security, while various component agencies also contribute to maritime security efforts, including U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and the Domestic Nuclear Detection Office (DNDO).<sup>1</sup> Key areas within maritime security include (1) port facility and vessel security; (2) maritime domain awareness and information sharing; and (3) international supply chain security. The Coast Guard is responsible for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, among other things, it conducts port facility inspections, leads the coordination of maritime information sharing efforts, and promotes domain awareness in the maritime environment. CBP is responsible for the maritime screening of incoming commercial cargo for the presence of contraband, such as explosives, while facilitating the flow of legitimate trade, cargo, and passengers. TSA and the Coast Guard have responsibility for the implementation and enforcement, respectively, of the Transportation Worker Identification Credential program to manage the access of maritime workers to regulated maritime facilities. DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including portal monitors. As one of the primary components responsible for maritime security protection, for fiscal year 2011 the Coast Guard had about 50,000 personnel, including civilian and military, and its budget authority was about \$10.2 billion.<sup>2</sup> Maritime

---

<sup>1</sup> U.S. Immigration and Customs Enforcement (ICE) also contributes to maritime security in that its mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks. In this capacity, ICE contributes to DHS border security efforts, including in the maritime environment, even though its main focus is not interdicting or screening operations.

<sup>2</sup> The budget and personnel figures for Coast Guard include its nonhomeland security related programs, such as its search and rescue mission function. In addition to Coast Guard resources, for fiscal year 2011 CBP had about 61,000 personnel and budget authority of about \$11.4 billion; TSA had about 55,000 personnel and budget authority of about \$7.7 billion; and the DNDO had about 130 personnel and budget authority of about \$340 million. However, the figures for these components include their nonmaritime security related programs for fiscal year 2011.

security primarily falls within the Quadrennial Homeland Security Review Mission 2: Securing and Managing our Borders.<sup>3</sup>

For the purposes of this report, we are generally focusing on key areas on which we and the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to maritime security also include maritime security national planning, we are not discussing DHS's progress and work remaining in this area. DHS has developed and implemented other efforts related to maritime security. For example, according to the Coast Guard, its maritime security programs are part of a layered strategy that begins far from our ports. Coast Guard officials noted that their security regime includes close coordination with international and regional organizations (such as the International Maritime Organization and the European Union), and individual country's coast guard equivalent agencies; security inspections of, and technical assistance to, foreign ports; and maintaining a multi-mission fleet of cutters patrolling our coastal approaches. The Coast Guard also noted that some of its other missions—those not directly part of its ports, waterways, and coastal security mission—can contribute to homeland security.

Further, in July 2011, the Coast Guard reported that it had specific initiatives underway to enhance maritime security planning at the port level, on which we have not previously reported. Specifically, Coast Guard reported that it had updated 43 port-level Area Maritime Security Plans that covered prevention, protection, security response, and short-term recovery, and that these plans were approved by Coast Guard district and area commanders. The Coast Guard further reported that it was working closely with maritime committees and stakeholders to maintain and annually exercise these port-level plans. We have not completed work on these areas upon which to make an assessment.

---

<sup>3</sup> While Coast Guard's maritime security efforts reported by us and the DHS IG primarily fall within Mission 2 of the Quadrennial Homeland Security Review, according to Coast Guard, its port level maritime security planning efforts fall within Mission 1: Preventing Terrorism and Enhancing Security and Mission 5: Ensuring Resilience to Disasters. For the purposes of this report, we discussed Coast Guard's port level security planning efforts under the maritime security functional area aligned under QHSR Mission 2, as discussed in appendix II on our scope and methodology.

---

## Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS's components, particularly the Coast Guard and CBP, have expanded their efforts in key areas, such as port facility and vessel security; maritime domain awareness and information sharing; and international supply chain security. The Coast Guard strengthened risk management through the development of a risk assessment model, and developed a strategy and programs intended to address risks to maritime facilities and passenger and commodity vessels. In addition, the Coast Guard increased maritime domain awareness through interagency operational centers, implementing a vessel tracking system, and identifying awareness gaps in the Arctic.<sup>4</sup> For example, in July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements resulting in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness. Further, in July 2011 DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments.

However, our work and that of the DHS IG has shown that more work remains. For example, DHS components' efforts to assess the effectiveness of programs to secure maritime facilities should be improved. We found that because of a lack of technology capability, DHS does not electronically verify identity and immigration status of foreign seafarers as part of its admissibility inspection process, thus limiting the assurance that fraud could be identified among documents presented by them. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, DHS and its partners should enhance efforts to improve maritime domain awareness by, for example, further strengthening tracking of small vessels. In addition, although DHS developed the Transportation Worker Identification Credential program, we found that the program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the

---

<sup>4</sup> Interagency operational centers are one element of maritime domain awareness, for which other agencies, particularly the Department of Defense, also have responsibilities.

Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Table 12 provides more detailed information on our assessment of DHS’s progress and work remaining in key areas on which we have reported, with an emphasis on work completed since 2008.

**Table 12: Assessment of Progress and Work Remaining in Key Maritime Security Areas on Which We Have Reported**

Area	Overall assessment	Summary of key progress and work remaining
Port facility and vessel security	<p>The Coast Guard strengthened security of port facilities and vessels by developing a risk assessment model; conducting annual inspections; working to prevent unauthorized entry of individuals; and providing additional efforts to secure passenger and commodity vessels. However, the information system for tracking inspections and efforts to assess the effectiveness of security measures should be improved.</p>	<p><b>The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. However, difficulties in calculating effects may challenge its ability to conduct risk assessments.</b></p> <p><b>Key progress:</b> The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. In July 2010 we noted that the Coast Guard made progress assessing risks by developing the Maritime Security Risk Analysis Model, which is used to assess risk to individual assets and facilities within ports. It is used by each Coast Guard sector, and assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios. The Coast Guard is starting to integrate the results of its risk assessment efforts into resource allocation decisions, including informing decisions about deployment of local assets. Additionally, the Coast Guard is starting to use the Maritime Security Risk Analysis Model results for evaluating capabilities needed to combat future terrorist threats and identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that the results of the risk assessments were used to refine the Maritime Security and Response Operations requirements for the number of cruise ship escorts and patrols of cruise ship facilities.<sup>a</sup> In July 2011, the Coast Guard reported that it had worked with DNDO to add radiological and nuclear threats to the Maritime Security Risk Analysis Model scenarios.</p> <p><b>What remains to be done:</b> We are conducting work examining the Maritime Security Risk Analysis Model, as well as reviewing the role that risk plays in the allocation of resources in the Port Security Grant Program.<sup>b</sup> In August 2011, we testified on the use of the Maritime Security Risk Analysis Model to assess offshore energy facilities. We found that the Coast Guard has several limitations in assessing the risks to such facilities. Such limitations involve calculating secondary economic effects and assessing the systematic or network risks of an attack on offshore energy facilities. We plan to report the results from our ongoing work later this year.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>DHS addressed risk to port facilities through annual inspections and efforts to prevent unauthorized entry of individuals. However, risks exist in not electronically verifying the identity and immigration status of foreign seafarers onboard cargo vessels.</b></p> <p><b>Key progress:</b> DHS has addressed risks to port facilities through annual inspections and programs designed to prevent the unauthorized entry of individuals. Federal law requires certain port facilities to have security plans in place.<sup>c</sup> Coast Guard guidance calls for at least one announced annual inspection and at least one unannounced annual spot check to ensure that plans are being followed. In February 2008, we reported that Coast Guard's inspections were identifying and correcting facility deficiencies. For example, the Coast Guard identified deficiencies in about one-third of the facilities inspected from 2004 through 2006, with deficiencies concentrated in certain deficiency categories, such as failing to follow facility security plans for access control. We are currently conducting work examining, among other things, the way in which the Coast Guard assesses risk and ensures security of offshore energy infrastructure.<sup>d</sup> As part of our review, we plan to analyze offshore infrastructure security plans and the Coast Guard's security inspection reports. We plan to report the final results from this effort later this year. In August 2011, we testified that the Coast Guard should strengthen its internal controls to ensure that required risk assessments are done at appropriate offshore infrastructure.</p> <p>Further, DHS took actions to address risks posed by unauthorized individuals with access to U.S. port facilities. Specifically, in January 2011, we reported on actions the Coast Guard and CBP took to address risk posed by foreign seafarers entering U.S. seaports. We found that the agencies were using a layered security strategy for identifying and addressing risks, and that CBP and the Coast Guard were conducting advance-screening, inspections, and enforcement operations. For example, both CBP and the Coast Guard received and screened advance information on commercial vessels scheduled to arrive at U.S. ports, and prepared risk assessments based on the results of the advance-screening of vessel and seafarer information. We also reported that the Coast Guard may conduct armed security boarding of arriving commercial vessels based on various factors, including intelligence it received to examine seafarer passports and visas, among other things, and ensure the submitted crew list is accurate.</p> <p>In addition, we have reviewed DHS's efforts to manage the access of maritime workers to regulated maritime facilities through the Transportation Worker Identification Credential program. For example, in May 2011, we reported that TSA designed processes to facilitate the issuance of credentials to maritime workers.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>What remains to be done:</b> With regard to foreign seafarers, in January 2011 we reported that because of a lack of technology capability, DHS did not electronically verify identity and immigration status on board cargo vessels, thus limiting assurance that fraud was identified among documents presented by foreign seafarers seeking admission into the United States. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, we reported that DHS faced challenges in ensuring it had reliable data on illegal entries by foreign seafarers at U.S. seaports. For example, both CBP and the Coast Guard track the frequency of absconder (a seafarer CBP has ordered detained on board a vessel in port, but who departs a vessel without permission) and deserter (a seafarer CBP grants permission to leave a vessel, but who does not return when required) incidents at U.S. seaports, but the records of these incidents varied considerably among the two agencies. As a result, the data DHS used to inform its strategic and tactical plans were of undetermined reliability. We recommended that DHS assess the risks of not electronically verifying foreign seafarers for admissibility, and that CBP and the Coast Guard determine why their data varied and jointly establish a process for sharing and reconciling records of illegal seafarer entries at U.S. seaports. DHS concurred and reported that CBP met with the DHS Screening Coordination Office to determine risks associated with not electronically verifying foreign seafarers for admissibility. Further, in July 2011 DHS reported that CBP and the Coast Guard were working to assess the costs associated with deploying biometric capabilities to the maritime domain. As these efforts are in the early stages, it is too soon to assess their results. Further, given the number of seafarers transiting U.S. ports each year and the continued threats posed by terrorism to the United States, establishing a process for sharing and reconciling information on absconder and deserter incidents could better support Coast Guard’s and CBP’s efforts to prevent illegal immigration at U.S. seaports.</p> <p>With regard to the Transportation Worker Identification Credential, in May 2011 we reported that program controls were not designed to provide reasonable assurance that only qualified applicants could acquire the credentials. For example, during covert tests of the Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Further, DHS had not assessed the program’s effectiveness at enhancing security or reducing risk for federally regulated facilities. We recommended, among other things, that DHS assess the program’s internal controls to identify needed corrective actions, assess its effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. DHS concurred and stated that it has initiated a review of current Transportation Worker Identification Credential program internal controls with a specific focus on the controls highlighted in our May 2011 report. As DHS is in the early stages of implementing these actions, it is too early to assess their impact. Until such efforts are completed, it will be difficult for DHS to provide reasonable assurance that the program is meeting its goals and that only qualified applicants can acquire the credentials.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>The Coast Guard conducted pre-entry security boarding, escorts, and patrols to secure passenger and commodity vessels, but additional actions and further study are needed.</b></p> <p><b>Key progress:</b> DHS took measures to help secure vessels including cruise ships, ferries, and energy commodity vessels such as tankers. In April and December 2010, we reported that DHS assessed risks to cruise ships and ferries, respectively, and in December 2007 we reported that DHS took action to prevent and be prepared to respond to attacks on energy commodity tankers. We also reported that DHS took measures to better secure these vessels. For example, the Coast Guard provided escorts for cruise ships to help prevent waterside attacks and a security presence on ferries during transit. CBP conducted reviews of passenger and crew data for terrorist connections or criminal ties and helped to ensure that all passengers and crew are cleared for entry into the United States. Further, with regard to energy commodity tanker security, the Coast Guard conducted security activities, such as pre-entry security boardings, escorts, and patrols.</p> <p><b>What remains to be done:</b> DHS made progress in these areas, but additional actions are needed to further enhance security. For example, we reported that CBP had not assessed the costs and benefits of requiring cruise lines to provide passenger reservation data for screening, which could help improve identification and targeting of potential terrorists. Additionally, Coast Guard records showed that at some ports, a lack of resources hindered some Coast Guard units from meeting their self-imposed requirements for activities, such as escorts and boardings to secure tankers. We recommended, among other things, that CBP conduct a study to determine whether requiring cruise lines to provide automated passenger data to CBP on a systematic basis would benefit homeland security. We also recommended that DHS develop a national resource allocation plan to balance the Coast Guard’s security responsibilities to protect energy commodity vessels with its other mission functions.</p> <p>DHS concurred with our recommendations and reported taking steps to address them. In July 2011, CBP reported that it had conducted site booking surveys at three ports of entry to assess the advantage of having cruise line booking data considered in a national targeting process, and had initiated discussions with a cruise line association on the feasibility of CBP gaining national access to cruise line booking data. Although CBP had originally set a due date of June 30, 2011, for its full evaluation of these issues, CBP reported that it had requested an extension to September 30, 2011, to obtain information from the cruise industry on potential impacts of requiring them to provide passenger data on a systematic basis. In addition, Coast Guard officials stated that they plan to develop a resource allocation plan, starting in April 2012, as part of the implementation of a national strategy, which is being developed for reducing the maritime security risks present in the bulk transportation and transfer of certain dangerous cargo on commodity vessels. In the interim, the Coast Guard has published guidance to clarify the process’ timing and scope to ensure full consideration is given to safety and security of the port, the facility, and the energy commodity vessel. We have reported that actions such as these are important to help ensure that the Coast Guard is positioning itself to address threats to passenger and commodity vessels. As CBP and the Coast Guard are in the early stages of implementing these efforts, it is too soon to assess their effectiveness.</p>

Area	Overall assessment	Summary of key progress and work remaining
Maritime domain awareness and information sharing	DHS strengthened maritime domain awareness through efforts such as establishing interagency operations centers, vessel tracking systems, and identifying security gaps in the Arctic. However, these efforts face challenges including budgetary constraints, difficulty tracking smaller and noncommercial vessels, and the need for improved information sharing with key Arctic stakeholders.	<p><b>DHS and its partners are working to establish interagency operations centers to improve maritime domain awareness, but these efforts face budgetary constraints and other challenges.</b></p> <p><b>Key progress:</b> The Security and Accountability For Every Port Act of 2006 calls for the establishment of interagency operations centers for port security, directing the Secretary of DHS to establish such centers at all high-priority ports no later than 3 years after the act's enactment (enacted October 13, 2006).<sup>e</sup> In October 2007, we reported that Coast Guard was piloting various aspects of future interagency operations centers at its 35 existing command centers and working with multiple interagency partners to further their development. According to the Coast Guard, future interagency operations centers would allow the Coast Guard and its partners to use port surveillance with joint tactical and intelligence information and share these data with port partners working side by side in expanded facilities.</p> <p>In July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements which resulted in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness.</p> <p><b>What remains to be done:</b> In October 2007, we reported that the Coast Guard faced budget constraints in trying to expand its current command centers and include other agencies at the centers. In our ongoing work looking at the continued implementation of Interagency Operations Centers, our preliminary observations indicate that as of August 2011, the Coast Guard has installed its information sharing system at more than 10 Coast Guard sectors.<sup>f</sup> Based on our preliminary observations, we identified concerns about whether the Coast Guard will meet its goals related to the involvement of port partners. We plan to report the final results of our work later this year.</p> <p><b>DHS implemented vessel-tracking systems, but tracking small vessels poses challenges.</b></p> <p><b>Key progress:</b> At sea or in U.S. coastal areas, inland waterways, and ports, the Coast Guard relies on a diverse array of vessel tracking systems operated by various entities. For tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system, and a commercially provided long-range automatic identification system.<sup>9</sup> For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system, and also either operates, or has access to, radar and cameras in some ports. In addition, in July 2011, DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. Among other things, DHS reported that this system would allow CBP to identify potential high-risk small boats to determine, for example, which needed to be boarded upon arrival.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>What remains to be done:</b> We identified limitations in the Coast Guard’s efforts to track vessels at sea. In March 2009, we reported that the means of tracking vessels at sea are potentially effective, but each has features that could impede its effectiveness. Also, the systems used in U.S. coastal areas, inland waterways, and ports—automatic identification system, radar, and video cameras—had more difficulty tracking smaller and noncommercial vessels because these vessels were not generally required to carry automatic identification system equipment, and because of the technical limitations of radar and cameras. To help address the small vessel threat, DHS developed a Small Vessel Security Strategy in April 2008, and in January 2011 issued the implementation plan for the strategy. As DHS is in the process of executing its implementation plan, it is too early to assess its effectiveness in enhancing maritime security.</p> <p><b>DHS identified and addressed some information gaps in the Arctic, but efforts would benefit from improved information sharing.</b></p> <p><b>Key progress:</b> In September 2010, we reported that, according to Coast Guard officials, establishing domain awareness in the Arctic would allow the Coast Guard to better understand the risks associated with operating in or monitoring the region, but that the Coast Guard faced obstacles to achieving domain awareness. Specifically, officials stated that establishing domain awareness was inhibited by (1) inadequate Arctic Ocean and weather data, (2) lack of communication infrastructure, (3) limited intelligence information, and (4) lack of a physical presence in the Arctic. The Coast Guard identified Arctic requirements and gaps for the maritime domain while also collecting relevant information from routine operations. For example, in September 2010 we reported that the Coast Guard established temporary operating locations in the Arctic and conducted biweekly Arctic overflights to obtain more information on the Arctic operating environment. In addition, information gathered during the Coast Guard’s routine missions, such as ice breaking and search and rescue, informed Coast Guard requirements for operating in the Arctic region.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>What remains to be done:</b> The Coast Guard’s success in implementing an Arctic plan rests in part on how successfully it communicates with key stakeholders, especially state and local officials, and Alaska Native tribal governments and interest groups. In September 2010 we reported that 9 of the 15 state and local officials we met with wanted more information on the status and results of the Coast Guard’s efforts to develop its future Arctic requirements. For example, some state and local officials believed that the agency had already determined its plan for Arctic operations but had not shared it, and one state official reported that his office and others may be willing to invest in infrastructure that could benefit the Coast Guard if and when they know the agency’s plans. Coast Guard officials told us that they have been focused on communication with congressional and federal stakeholders and intended to share Arctic plans with other stakeholders once plans are determined. In the interim, some state and local stakeholders reported having limited information that they believe would be useful on the process and progress of the agency’s Arctic planning efforts. We recommended that the Coast Guard communicate with key stakeholders on the process and progress of its Arctic planning efforts. DHS concurred and in July 2011 reported it was taking actions to address our recommendation, such as soliciting comments from indigenous populations and the public on the National Ocean Policy and participating on the International Arctic Council, a high-level forum for promoting cooperation, coordination, and interaction among Arctic nations, indigenous communities, and other Arctic stakeholders on Arctic issues.<sup>h</sup> While these are positive steps, it is too early to assess the outcomes of DHS’s consultation efforts.</p>
International supply chain security	DHS made progress in deploying container screening technologies and partnered with foreign governments for supply chain security. However, these efforts would be enhanced by the development of measures to assess the performance of new technologies and the completion of a feasibility analysis of implementing the requirement to scan 100 percent of all U.S.-bound cargo containers.	<p><b>CBP made progress in deploying new technologies, but development and implementation of these technologies should be improved through performance standards and alignment with operational needs.</b></p> <p><b>Key progress:</b> DHS has made progress in developing technologies to improve container security by detecting intrusions and tracking containers and scanning them for contraband, including nuclear material. DHS conducted research and development for four container security technology projects to detect intrusion and track the movement of containers through the supply chain. For example, DHS’s Science and Technology Directorate initiated the Container Security Device project to develop the capability to detect container door intrusion. Further, to detect nuclear materials, CBP, in coordination with DND, 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 alarm when they detect radiation coming from a package, 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.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>What remains to be done:</b> We reported in September 2010 that DHS had not yet developed performance standards for these new technologies because it had not yet demonstrated that they can effectively work in operational environments. Additionally, DNDO began working on the cargo advanced automated radiography system with the intention that this technology could be used to detect a variety of contraband, including shielded nuclear materials, in vehicles and containers at U.S. ports of entry. However, we reported that the office did so without fully understanding that the technology would not fit within existing primary inspection lanes at CBP ports of entry.<sup>1</sup> We identified lessons learned for DHS to consider in its future acquisition efforts, such as to (1) engage in a robust departmental oversight review process, (2) separate the research and development functions from acquisition functions, (3) determine the technology readiness levels before moving forward to acquisition, and (4) rigorously test devices using actual agency operational tactics before making decisions on acquisition. DHS announced the termination of the program in September 2010.</p> <p>DNDO also tested next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials. We reported in June 2009 that while DNDO increased the rigor of testing the new monitors in comparison with previous tests and thereby added credibility to the test results, the benefits of the monitors may not justify the high cost. In July 2011, the Director of DNDO testified that because the original design specification for advanced spectroscopic monitors program does not adequately reflect the operational needs in the field, and because there are now competing commercially-available portal radiation detection systems, DHS was ending the program as originally conceived. DHS reported that it plans to deploy the existing units to field locations to gather operational data to support future planning efforts.</p>

Area	Overall assessment	Summary of key progress and work remaining
		<p><b>DHS developed and implemented programs to partner with foreign governments to inspect suspicious cargo before it leaves for U.S. ports, but these programs should be improved through enhanced planning such as feasibility analyses and oversight.</b></p> <p><b>Key progress:</b> DHS implemented programs to inspect suspicious cargo before it leaves for U.S. seaports. For example, CBP established partnerships with members of the international trade community, including the private sector through its Customs-Trade Partnership Against Terrorism, and with foreign governments through its Container Security Initiative and Secure Freight Initiative. The Container Security Initiative program places CBP staff at participating foreign ports to partner with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States, and the Secure Freight Initiative is a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas. DHS reported that, as of July 2011, the Container Security Initiative was operational at 58 ports worldwide. CBP and its international partners also developed the World Customs Organization’s Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework). In February 2010, the DHS IG reported on CBP’s management and oversight of the Container Security Initiative program. The DHS IG noted that CBP had used proactive management and oversight processes through the Container Security Initiative to identify and inspect high-risk cargo at foreign ports. The IG further reported that CBP conducts periodic evaluations of overseas Container Security Initiative operations and has software tools to help managers monitor port activities.</p> <p><b>What remains to be done:</b> We reported in October 2009 that CBP had made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative program, leaving the feasibility of 100 percent scanning largely unproven. CBP had not developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.<sup>1</sup> Among other things, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning of all U.S.-bound cargo containers in light of the challenges faced at the initial Secure Freight Initiative ports. DHS concurred with our recommendations. Although DHS has not conducted a feasibility analysis, DHS reported that it is examining alternatives to 100 percent scanning as part of the current effort to develop the National Strategy for Global Supply Chain Security, which is intended to articulate an integrated U.S. government vision for collaborating broadly to manage the risks presented by and to the global supply chain. According to DHS, this strategy is undergoing interagency review, and should be issued in the fall of 2011. This strategy should help DHS more fully evaluate various alternatives for implementing the 100 percent scanning requirement or other alternatives that enhance cargo container security in a cost-efficient manner. However, since the strategy is not yet complete, it is too early to assess its impact.</p>

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

<sup>a</sup> Maritime Security and Response Operations requirements were referred to Operation Neptune Shield requirements until November 2010. They require Coast Guard units to escort a certain percentage of high capacity passenger vessels at each maritime security threat level to protect against an external threat, such as a waterborne improvised explosive device. This requirement is applicable to all types of high capacity passenger vessels—cruise ships, ferries, and excursion vessels—in a sector’s area of responsibility.

<sup>b</sup> We are conducting our work for the Senate Committees on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and the House Homeland Security Committee, Subcommittee on Border and Maritime Security.

<sup>c</sup> The Maritime Transportation Security Act of 2002, as amended, establishes requirements for various layers of maritime security, including requiring a national maritime transportation security plan, area maritime transportation security plans, and facility and vessel security plans. The act calls for various types of facilities to develop and implement security plans, and it places federal responsibility for approving and overseeing these plans with DHS. See Pub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2068 (2002) (codified as amended at 46 U.S.C. § 70103). DHS has placed lead responsibility for this and other Maritime Transportation Security Act requirements with the U.S. Coast Guard. Subsequent Coast Guard guidance called for conducting annual on-site inspections and annual unannounced spot checks to verify a facility’s compliance with its security plan.

<sup>d</sup> We are conducting our work for the House Committee on Homeland Security and its Subcommittee on Oversight, Investigations and Management; the House Committee on Energy and Commerce; the House Committee on Transportation and Infrastructure; the Senate Committee on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and Representative Edward Markey.

<sup>e</sup> See Pub. L. No. 109-347, § 108(a), 120 Stat. 1884, 1892 (2006) (codified as amended at 46 U.S.C. § 70107A).

<sup>f</sup> We are conducting this work for the Senate Committee on Commerce, Science, and Transportation; the House Committee on Transportation and Infrastructure; and the Senate Committee on Homeland Security and Governmental Affairs.

<sup>g</sup> The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the *International Convention for the Safety of Life at Sea, 1974*. In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

<sup>h</sup> The National Ocean Policy is policy adopted by executive order that includes a set of overarching guiding principles for management decisions and actions toward U.S. oceans, coasts and the Great Lakes. Exec. Order No. 13,547, 75 Fed. Reg. 43,023 (July 19, 2010).

<sup>i</sup> DNDO announced the termination of the Cargo Advanced Automated Radiography System program in September 2010.

<sup>j</sup> See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

---

## GAO Contact

For additional information about this area, contact Stephen L. Caldwell at (202) 512-9610 or [caldwells@gao.gov](mailto:caldwells@gao.gov).