GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 22, 2010

The Honorable John D. Rockefeller IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

Subject: *Maritime Security: Responses to Questions for the Record*

On July 21, 2010, we testified before your committee on the Department of Homeland Security's (DHS) progress and challenges in key areas of port security.[1] Members of the committee requested that we provide additional comments to a number of post hearing questions. The questions and our answers are provided in the Enclosure 1. The responses are based on work associated with previously issued GAO products and also include selected updates—conducted in September 2010—to the information provided in these products. We conducted this work in accordance with generally accepted government auditing standards. To ensure the technical accuracy of the updated information obtained in September 2010, we provided of copy of the information contained in this letter to DHS. DHS provided technical comments that we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, this letter will be available at no charge on the GAO Web site at http://www.gao.gov.

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

If you have any questions about this letter or need additional information, please contact me at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this letter. Key contributors to this letter are listed in Enclosure 2.

Stephen L. Caldwell
Director
Homeland Security and Justice

Enclosures

Enclosure 1

GAO Responses to Questions for the Record

Small Vessel Threats and Strategy

Question from Chairman Rockefeller

1. **Pending the release of the implementation plan for the DHS Small Vessel Security Strategy, what are the potential options for mitigating threats from small vessels? To what extent would a new requirement that small vessels carry transponders—so they could be tracked—be a viable solution? How does this option compare to increased "neighborhood watch" type programs to encourage watermen and pleasure boaters to report suspicious activity?**

Please see question 2 below for a joint response.

Question from Senator Hutchison

2. **Since the terrorist attacks of September 11, 2001, maritime security efforts have focused primarily on large commercial vessels, cargoes, and crew. Efforts to address the small vessel environment have largely been limited to traditional safety and basic law enforcement concerns. Small vessels are, however, readily available for potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, other contraband, and other criminals. Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs). GAO previously noted that technology systems used by the Coast Guard to track small vessels have not worked properly at night or during inclement weather. In your view, is it cost-effective to track small vessels?**

Governmental agencies, both in the United States and abroad, have exercised several options to address the risks presented by small vessels. As we previously reported in April 2010,[2] the Department of Homeland Security (DHS)—including the U.S. Coast Guard and U.S. Customs and Border Protection (CBP)—and other entities are taking actions to reduce the risk from small vessels. These actions include the development of the *Small Vessel Security Strategy*,[3] community outreach efforts through the America's Waterway Watch (AWW) program and Operation Focused Lens, port-level vessel tracking efforts with radars and cameras, port-scale nuclear detection pilot projects,

[2] GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400, (Washington, D.C.: Apr. 9, 2010).

[3] The goals of DHS's *Small Vessel Security Strategy* are consistent with the critical infrastructure protection maritime sub-sector goal to enhance the resiliency of the maritime transportation system. According to the strategy, reducing the risk from small vessels will contribute to the security of our ports and help prevent the disruption of commerce and the negative impact of a vessel security incident by reducing the potential consequences of such an incident. The primary consequence of a terrorist incident (as well as other transportation security incidents) arising from the use of a small vessel could be devastating for the U.S. economy if it damaged critical infrastructure or resulted in closure of a port. By reducing the risk and the associated consequences from small-vessel risks, the strategy contributes to the resilience of the maritime sector and associated critical infrastructure.

establishment of security zones in U.S. ports and waterways, and escorts of possible targets of waterborne improvised explosive devices. CBP and the Coast Guard also have other efforts under way to prevent small vessels from transporting weapons of mass destruction, terrorists, or narcotics from foreign countries into the United States. CBP's Office of Air and Marine reports that it is using airborne assets such as four engine P3 Airborne Early Warning and Long Range Tracker aircraft and soon maritime reconnaissance versions of unmanned Predator drones, to detect smugglers' vessels, including semisubmersibles, sailing to the United States. The Coast Guard and CBP's Office of Air and Marine also report that they station patrol vessels along smuggling routes to intercept smugglers' vessels before they reach U.S. shores. At the request of Chairman Bennie Thompson and Ranking Member Peter King of the Committee on Homeland Security, House of Representatives, we are currently reviewing CBP's Office of Air and Marine program and examining the agency's use of its resources and expect to issue the results of this review next year. Outside of the United States, the government of Singapore began a program in 2007 called Harbour Craft Transponder System where all vessels not covered by the International Maritime Organization's (IMO) International Convention for the Safety of Life at Sea (generally, this convention covers vessels 300 gross tons or more on an international voyage and cargo ships of 500 gross tons or more) were required to install and operate transponders that broadcast their position. The program was implemented jointly by the Maritime and Port Authority, the Police Coast Guard and the Republic of Singapore Navy, and an estimated 2,800 small vessels were equipped when its operation commenced in 2007. User costs include the transponder device, which ranges in cost from approximately $700 to $730 plus applicable taxes, depending on whether the model is portable or fixed, and an annual operating cost of approximately $90.

As we reported in March 2009, the expansion of vessel tracking to all small vessels—through transponders or other methods—may be of limited utility because of the large number of small vessels, the difficulty identifying threatening actions, the challenges associated with getting resources on scene in time to prevent an attack once it has been identified, and the limitations of certain equipment.[4] For vessels not required to carry automatic identification system (AIS)[5] equipment, cameras may be utilized, though not all ports have cameras suited to overcome challenges posed by low lighting during operation at night or in bad weather. Even when vessels carrying transponders are tracked in ports, recognizing hostile intent is very difficult. During our reviews of maritime security efforts, we were provided evidence of vessels intruding into security zones where unauthorized access was prohibited. While no attacks occurred, such vessels were able to travel freely near potential targets. Coast Guard officials have told us that their ability to enforce security zones is constrained by their limited resources. Moreover, the Coast Guard has not been able to meet its own internal standards for the frequency of escorts of potential target vessels. The difficulty in recognizing potentially

[4] As we reported in March of 2009, some cameras have the ability to operate in low light or use infrared images that distinguish objects by the heat they emanate. These capabilities allow them to be effective when cameras using visible light prove ineffective, such as at night or in bad weather. However, these cameras can still be affected by high surf conditions, which can hide vessels smaller than the height of the waves. For additional information, see GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

[5] AIS is a technology that uses global navigation satellite data and radios to transmit and receive information about a vessel's voyage, including its name, position, course, and speed.

threatening activity and the limited response capability indicates that expanding tracking to all small vessels would not necessarily diminish the risk posed by small vessels. While such tracking would likely lead to increased observation of prohibited activities, such as intrusion into security zones, it would not necessarily help to differentiate between vessels that entered security zones with hostile intent and vessels that entered for other reasons, such as better fishing. In addition, with the increased number of vessels to observe, watch standers could be overwhelmed by the amount of information they must track or monitor. While the Coast Guard has research underway to automate its ability to detect threatening behavior by vessels, even if these efforts are successful they would not improve the agency's ability to respond quickly. DHS's *Small Vessel Security Strategy* also states that small-vessel risk reduction efforts should not impede the lawful use of the maritime domain or the free flow of legitimate commerce—making the need to decipher vessel behavior essential. As the strategy states, given the size and complexity of the maritime domain, risk-based decision making is the only feasible approach to prevention, protection, response and recovery related to small-vessel threats.

Much of the seaborne smuggling of narcotics and undocumented migrants into the United States currently makes use of small vessels, such as high-speed "go fast" boats and semisubmersibles. While CBP and the Coast Guard are also taking actions to intercept smugglers at sea, their ability to prevent this smuggling is mixed. In its fiscal year 2009 performance report, the Coast Guard reported removing 15 percent of the cocaine being transported on noncommercial vessels bound for the United States in fiscal year 2009. Conversely, the Coast Guard reported that it interdicted approximately 84 percent of undocumented migrants who attempted to enter the United States via maritime routes in fiscal year 2009. CBP's performance report did not include similar measures for maritime narcotic or migrant interdiction.

With the critical task of mitigating the risk posed by small vessels before the Coast Guard and CBP, we believe a risk management approach coupled with strong intelligence-gathering efforts would lead to the greatest benefit. Intelligence-gathering efforts at the port level, such as AWW, should help uncover potential threats before they develop into full-fledged attacks. The program's outreach to over 400 local watch group members in and around the Puget Sound region for the Vancouver 2010 Winter Olympics demonstrated its potential as means of increasing vigilance and communication. Moreover, targeted efforts aimed at protecting critical infrastructure and valuable vessels, along with random escorts and patrols, should help provide deterrence against a small vessel attack inside U.S. port areas. Offshore, intelligence efforts aimed at uncovering smuggling operations should also help to target patrols and interceptions. These efforts would include random patrols, which add uncertainty to where these assets will be at any one time. A risk management approach that focuses limited resources on the greatest risks is even more critical given the federal government's current budget climate.

Security in Overseas Ports

Questions from Chairman Rockefeller

3. Regarding security in foreign ports, your statement emphasized the importance of risk management and indicated that your work had shown potential to apply more risk management to the Coast Guard inspection of foreign ports. What did your work specifically show and how could the Coast Guard use risk management more effectively? Can the Coast Guard do this on its own, or would legislative changes be needed to implement changes in the frequency or intensity of visits to foreign ports?

Since we issued our report on the Coast Guard's International Port Security Program in April 2008, the Coast Guard has adopted a new risk management program.[6] In April 2008, the Coast Guard was just beginning the next phase of the program, revisiting countries to reassess the security measures of 138 trading partners. As part of this next phase, the Coast Guard planned to place greater emphasis on countries that were not in compliance or that were struggling to comply with International Ship and Port Facility Security (ISPS) Code requirements. To accomplish this with available resources, the Coast Guard planned to prioritize its country visits and capacity-building efforts using a risk-based approach that would allow Coast Guard officials to spend more time in countries not in compliance and whose lack of compliance poses a higher risk to the United States. At the time of our report, the Coast Guard was in the process of developing this risk-management approach and had created working groups to consider how to implement this approach. Since the issuance of our report, the Coast Guard reported that the program finalized its methodology which analyzes the risk a country potentially poses to the United States, how well a country is implementing the ISPS Code, and the likelihood that capacity-building efforts in the country would be effective considering a variety of political, economic, and social preconditions. According to the Coast Guard, the results of the methodology are used to manage risk and limited resources by helping establish assessment team size, determining countries and ports where capacity-building resources would be most effective, and finally identifying high-risk countries that need additional oversight. We have not conducted a detailed review of this methodology or the Coast Guard's implementation of it.

Although we have not analyzed or directly reported on this issue as it relates to the Coast Guard, another approach the Coast Guard could consider to incorporate risk management into the program is to use mutual recognition arrangements with other countries, similar to that developed by CBP for international customs. We reported in August 2008 that CBP worked with the international customs community to achieve a system of mutual recognition—an arrangement whereby the actions or decisions taken by one customs administration are recognized and accepted by another administration.[7] For a system of mutual recognition to work, however, there must be an agreed-upon common set of standards that are applied uniformly so that a level of confidence exists between countries. As international standards exist for maritime security through the

[6] Our April 2008 report is restricted and not available to the public.

[7] GAO, *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standard and Initiatives, but Challenges Remain*, GAO-08-538 (Washington, D.C.: Aug. 15, 2008).

ISPS Code, the Coast Guard could consider developing a similar system of mutual recognition for international maritime security. For example, the European Union has developed detailed regulations for the consistent implementation of the ISPS Code by its member states and established a process for verifying the effectiveness of its member states' maritime security measures. This process includes an inspection of member states' ports that results in a report identifying any nonconformities with the regulations and making recommendations to address the nonconformities. Should the Coast Guard develop confidence in the European Union's regulatory and inspection approach to determine whether its members have fully implemented and maintain international maritime security standards, under a mutual recognition arrangement with the European Union the Coast Guard could agree to recognize and accept one another's security practices. The Coast Guard could then give countries with which it has such agreements lower priority for a country visit. During a meeting in September 2010 to follow-up on our report, Coast Guard officials told us that more flexibility to determine whether an assessment is necessary for countries with which there is confidence in the implementation of international maritime security standards would be helpful to the program in allocating program resources toward the highest-risk countries. Changes to increase the frequency of visits to foreign ports would not require a legislative change, whereas a decrease in frequency may require a legislative change.

In regard to the Coast Guard's ability to spend more time in countries not in compliance to assist with capacity building, we reported in April 2008 that the International Port Security Program was subject to limitations on its ability to offer capacity-building assistance outside of assessment activities or to other countries that may comply with the ISPS Code standard, but struggle to maintain their compliance. Coast Guard officials stated that while authorities allowed for certain types of capacity-building activities, several of the authorities limited those activities to ports in foreign countries that have been found to lack effective antiterrorism measures. However, with the enactment of the Coast Guard Authorization Act of 2010,[8] the Coast Guard has new authorities to provide assistance to what the Coast Guard describes as a broader range of countries. For example, the act authorizes the Coast Guard to provide specified types of assistance to foreign ports based on risk assessments and comprehensive port security assessments rather than a finding of the lack of effective antiterrorism measures before providing assistance. In terms of changes to the frequency of visits to foreign ports, although the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) currently requires that a minimum number of reassessments of the effectiveness of antiterrorism measures in foreign ports be conducted at a rate of not less than once every 3 years,[9] the International Port Security Program strives to conduct reassessments every 2 years to follow the direction contained in the conference report accompanying the fiscal year 2007 DHS Appropriations Act.[10] The Coast Guard states that in addition to the reassessments, it visits all countries at least annually, with countries that have ports with nonconformance issues it has identified more frequently. Consequently, to decrease the frequency of visits to an amount less than the established frequencies in the SAFE Port Act would require legislative changes whereas an increase in frequency would not require legislative changes.

[8] Pub. L. No. 111-281, ___ Stat. ___ (2010).
[9] Pub. L. No. 109-347, 120 Stat. 1884, 1918 (2006).
[10] H.R. Conf. Rep. No. 109-699, at 142 (2006).

4. S. 3639 authorizes the Coast Guard to provide assistance to foreign governments or ports to enhance their maritime security. Does GAO support this provision?

The provisions in S. 3639 to authorize the Coast Guard to provide assistance to foreign governments or ports to enhance their maritime security are similar to provisions recently enacted in the Coast Guard Authorization Act of 2010. While we have not directly looked at this issue, based on our work, Coast Guard technical assistance to other countries could be another way to improve port security in certain circumstances with available Coast Guard resources. During our review of the International Port Security Program, Coast Guard officials told us that funding is a major challenge for most countries struggling to meet and sustain ISPS Code requirements.[11] For example, Coast Guard officials stated that in several African countries, the designated authority within the government does not have the resources to provide security for ports or funds to provide grants for ports in need of improvements. However, according to Coast Guard officials, the Coast Guard also does not have resources to supply physical security assets, such as fences and guards, to those countries that cannot afford them. Program officials have sought to raise awareness about low-cost methods that can be used to meet certain international security requirements, such as the use of "tabletop" exercises rather than conducting full-scale drills and exercises.

In addition to the budgetary limitations, Coast Guard officials stated that the program faced legal limitations in the capacity-building efforts they could provide under their previous legislative authorities. As discussed above, while previous authorities allowed for certain types of capacity-building activities, several of those authorities limited those activities to ports in foreign countries that had been found to lack effective antiterrorism measures. However, with the enactment of the Coast Guard Authorization Act of 2010, the Coast Guard has new authorities to provide assistance. For example, the act authorizes the Coast Guard to provide assistance based on risk assessments and comprehensive port security assessments rather than a finding of a lack of effective antiterrorism measures. Another capacity-building authority authorizes the provision of technical assistance when it is provided in conjunction with regular Coast Guard operations. The Coast Guard Authorization Act of 2010 amended this authority to expressly authorize the use of funds for certain purposes such as the activities of traveling contact teams, including any transportation expense, translation services, seminars, and conferences involving members of maritime authorities of foreign governments, and the distribution of publications pertinent to engagement with maritime authorities of foreign governments.

5. Does the Coast Guard have an adequate workforce of inspectors who can operate in foreign environments to inspect foreign ports? To what extent would that workforce be affected by proposals to change the frequency or intensity of visits to foreign ports? How would it be affected by proposals to increase technical assistance to foreign governments and ports outside of the normal visit/inspection cycle?

We reported in January 2010 that during this decade, the Coast Guard has been challenged with expanded mission responsibilities, and concerns have been raised about

[11] Our April 2008 report is restricted and not available to the public.

whether the Coast Guard has a sufficient workforce to fulfill these mission responsibilities.[12] The impact of expanding missions underscored shortcomings in the Coast Guard's ability to effectively allocate resources, such as personnel; ensure readiness levels; and maintain mission competency. Similarly, when we concluded our review of the International Port Security Program in April 2008, we reported that the Coast Guard also faced challenges in ensuring that it had trained staff available to meet assessment and assistance needs. According to Coast Guard officials, personnel working in the program have unique demands placed on their skills since they must be proficient security inspectors and must also be culturally and diplomatically sensitive liaisons to foreign countries. The challenge was made more difficult by Coast Guard plans to compress its schedule for completing follow-up visits so that all were to be completed within a 2-year time frame and by the Coast Guard personnel rotation policy that moves personnel between different positions every 3 to 4 years.

We also reported that the Coast Guard did not have a fully developed strategic workforce plan for the program. Coast Guard officials noted that the calculations for the number of program personnel required were straightforward as the number of countries to assess was limited to approximately 138 and the amount of time required to conduct assessments was known. When we asked Coast Guard officials about ensuring the availability of sufficient resources for the next phase of the program, Coast Guard officials stated that they believed they had sufficient resources to conduct assessments and provide capacity building within the current authorities provided to the program. However, we reported that they had not completed aspects of workforce planning, such as processes to regularly analyze staffing data and workforce demographics and develop strategies for identifying and filling gaps, as human capital management guidance provided by the Office of Personnel Management suggests. Without such planning, we reported that it may be difficult for the Coast Guard to meet its program goals. As a result, we recommended that the Coast Guard develop and incorporate a workforce plan as part of the risk management approach it was developing to prioritize the performance of program activities. DHS and the Coast Guard concurred in part with our recommendation. Specifically, they noted that the Coast Guard has analyzed its workforce needs to carry out the functions currently mandated and had begun to develop a methodology to determine where best to conduct capacity-building efforts. They stated that more analysis would be done when and if authorities are provided to expand the capacity-building activities of the program. While we agreed that the Coast Guard would need additional authorities to carry out certain capacity-building activities beyond countries not in compliance, the Coast Guard's workforce planning efforts were not consistent with those called for by human capital management guidance, even for the program's current authorities.

While we do not have the data or information to determine how the Coast Guard's workforce would be affected by potential changes to the frequency or intensity of visits, or changes to increase the technical assistance to foreign governments and ports, since the issuance of our report the Coast Guard has reported taking additional actions to more fully develop a workforce plan for the program. Although the program does not envision a separate "stand-alone" plan, the Coast Guard reported reviewing human capital management guidance and is incorporating some of the principles in its program

[12] GAO, *Coast Guard: Service Has Taken Steps to Address Historic Personnel Problems, but It Is too Soon to Assess the Impact of These Efforts*, GAO-10-268R, (Washington, D.C.: Jan. 29, 2010).

management. Among other things, the Coast Guard reported that the program continues to refine its human capital management including using an analysis to identify training needs for new personnel entering the program and promulgation of guidance on resources that should be devoted to conducting assessment visits for various categories of countries. The program also reported finalizing its methodology which looks at the risk a country potentially poses; how well it is implementing the international security standard, the ISPS Code; and the likelihood that the capacity-building efforts in the country would be effective. While we have not assessed these actions, we believe they contribute towards the implementation of our recommendation and thereby better position the Coast Guard to ensure that it has an adequate workforce. Should the program be given additional capacity-building authority, the Coast Guard stated that the program will use its methodology to identify additional personnel needs and where they should best be stationed.

Question from Senator Klobuchar

6. **As recently as this month, the U.S. Coast Guard estimated that as many as 15 countries are not maintaining effective antiterrorism measures at their port facilities. If foreign ports or facilities fail to maintain these measures, the Coast Guard has the authority to deny entry to vessels arriving from such ports or impose specific conditions on the vessels in order to be allowed entry to the U.S. Can you tell us more about this assessment and what the conditions on the ground are at these ports? How are we working with foreign governments to increase protective measures at their ports? What steps are we taking to address the national sovereignty concerns of nations whose ports are being examined under the International Port Security Program?**

There are a variety of reasons and circumstances whereby the Coast Guard deems a country and its ports as not in compliance with international port security standards. In regards to the conditions in countries currently considered not to be maintaining effective antiterrorism measures at their port facilities, the Coast Guard considers this information as sensitive and it therefore cannot be publicly released. However, the Coast Guard told us that its concerns about these countries generally center around the failure of the contracting government to audit the ISPS Code compliance of its port facilities and on the individual port facilities' failure to adequately control access of personnel and cargo. During the assessment the Coast Guard conducts of foreign ports[13] through its International Port Security Program, Coast Guard officials visit and review the implementation of security measures in foreign ports, examining the physical security measures and access controls at the ports as well as the policies, procedures, and training related to the ISPS Code. Based on its visit and the information provided by the foreign country, the Coast Guard team determines the extent to which the country has substantially implemented the ISPS Code. The Coast Guard team makes a determination

[13] While the focus of the program is country based, the implementation status of specific ports or port facilities is considered on a case-by-case basis if the country has not substantially implemented the ISPS Code. In certain cases, a port facility that has implemented the ISPS Code in a country that has not may request that it be considered separately from the country. Requests are handled on a case-by-case basis and are generally limited to only those port facilities critical to maritime trade with the United States based on factors such as the volume and importance of the cargo imported from or exported to that port or port facility.

that a country has "substantially implemented" the ISPS Code if the team concludes that effective security measures are in place at the ports that meet the requirements of the ISPS Code and the government exercises effective oversight. If the team does not observe these items, the team makes a determination that the country "has not substantially implemented" the ISPS Code. In addition to being an outcome of a country visit, the Coast Guard may also find a country to not have substantially implemented the ISPS Code if it denies access to its ports, it fails to communicate information on its compliance to the Coast Guard or the IMO, or a credible report by another U.S. government agency or other source finds that substantial security concerns exist.

In cases where a country has been found not to have substantially implemented the ISPS Code, the Coast Guard explains the identified deficiencies and makes recommendations to the country for addressing the deficiencies and provides possible points of contact for assistance to help the country improve. In addition, Coast Guard officials work with the appropriate American embassy to identify other capacity-building resources that might assist the country. As part of the program, the Coast Guard has been collecting and sharing best practices it has observed during its visits with a special emphasis on low-cost security practices or innovative applications that are easy to implement and do not require a significant financial investment. The Coast Guard shares these best practices with other countries and makes them publicly available through the program's Web site to assist foreign governments in making improvements in their port security. The Coast Guard team then revisits the country to observe whether identified deficiencies have been addressed. Depending on the progress observed and the cooperation received from the country, the team may decide to continue to work with the country and make a revisit or place conditions on vessels that try to enter U.S. ports after visiting the country's ports. During our review, Coast Guard officials cited their efforts in one Caribbean Basin country as an example of how the Coast Guard works with foreign governments to increase protective measures at their ports. In that case, the Coast Guard initially found that ports in the country were not substantially implementing the ISPS Code. After several rounds of sharing information on security training, discussions of best practices for security exercises, and suggestions for specific physical security improvements, the Coast Guard found that the country had made substantial progress toward implementing the ISPS Code.

In regards to national sovereignty concerns, the Coast Guard is aware of such concerns and has considered ways to address them. The Coast Guard has stated that because of sovereignty concerns and "assessment fatigue," it is becoming increasingly difficult to gain access to countries such as China, Egypt, India, Libya, Russia, and Venezuela for reassessments. During our review, Coast Guard officials stated that an effort was underway to conduct joint visits when possible with other U.S. government agencies as well as increase the sharing of assessment data among various agencies to reduce the "footprint" of U.S. government activities in the countries. As another approach, Coast Guard officials stated that they have also considered partnering with other foreign governments and international organizations to complete assessments. However, the Coast Guard has not partnered with any international governments to conduct reassessments because the international community has not developed an approach or methodology as the Coast Guard has for inspecting ports. The Coast Guard has also reported that it works frequently with international organizations such as the Asia Pacific Economic Cooperation (APEC) and the Organization of American States on capacity-building projects and utilizes the information obtained when conducting such

actions as part of the assessment process. For example, as part of APEC's Transportation Working Group's maritime expert group security subcommittee, the Coast Guard assisted in creating the Port Security Visit Program and has participated in several of the assessment visits to member economies. In addition, the Coast Guard has conducted joint visits with auditors from the Secretariat of the Pacific Community in Pacific island nations. In the short term, program officials stated that the best way to mitigate a possible lack of cooperation from sovereign nations is to continue to reach out and diplomatically work with countries. The recently enacted Coast Guard Authorization Act of 2010 now mandates that unless the Coast Guard finds that a port in a foreign country maintains effective antiterrorism measures, that the Coast Guard notify appropriate governmental authorities of the foreign country and allows the imposition of conditions of entry (requiring vessels to take additional security measures) "unless the Coast Guard finds effective anti-terrorism measures in place in foreign ports." In cases where countries still deny the Coast Guard access to their ports, program officials will implement and utilize these provisions as required and work with other Coast Guard programs in the domestic arena—specifically, programs that examine foreign vessels to verify their compliance with ISPS Code requirement—and conduct offshore security boardings of vessels to help limit the access of high-risk vessels to U.S. ports.

Port Security Grant Program

Question from Senator Lautenberg

7. The Port Authority of New York and New Jersey is unable to move forward on a number of projects to improve the security of the port because of the twenty-five percent cost share requirement for port security grants. It is my understanding that waiving this requirement is a long, arduous process that is rarely successful. What should be done about this cost-share requirement so that it does not impede the security of our ports?

Matching contributions—also known as cost-share requirements—are a key factor for effective federal grants for two reasons. First, it is important that federal dollars are leveraged to ensure that federal grants supplement stakeholder (whether public or private) spending rather than serve as a substitute for stakeholder spending on grant-funded projects. If a grant program is not designed to encourage supplementation, other stakeholders may rely solely on federal funds and choose to use their own funds for other purposes, meaning that federal funds cannot be leveraged to the extent they otherwise could be. We reported in September 2003 that the inclusion of matching requirements is one method through which to encourage supplementation of federal grants.[14] Second, matching requirements are reasonable given that grant benefits can be highly localized. For example, regarding port security grants, we reported in December 2005 that,

> "Ports can produce benefits that are public in nature (such as general economic well-being) and distinctly private in nature (such as generating profits for a particular company). The public benefits they produce can also be distinctly local in nature, such as sustaining a high level of economic activity in a particular state

[14] GAO, *Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs*, GAO-03-1146T (Washington, D.C.: Sept. 3, 2003).

> or metropolitan area. Thus, state and local governments, like private companies, also have a vested interest in ensuring that their ports can act as efficient conduits of trade and economic activity. Given that homeland security threats can imperil this activity, it can be argued that all of these stakeholders should invest in the continued stability of the port."[15]

However, in the December 2005 report, we also recognized the differences of opinion among policymakers regarding the inclusion of matching requirements in federal grants. Some might see substitution of federal funds for local funds as reasonable given differences in fiscal capacity, while others may view homeland security as a shared responsibility. For policymakers who place greater value on reducing the substitution of federal funds for local funds, strengthening matching requirements offers one option in administering grants. One way to implement this requirement involves using a sliding scale for matching federal funds depending on the fiscal capacity of the grant applicant. Additionally, the matching requirement under the fiscal year 2009 Port Security Grant Program (PSGP) stated that the match may be in the form of cash or in-kind contributions, allowing grant recipients flexibility in meeting this requirement. However, the cost-share requirement was waived for fiscal year 2010 port security grants.

Aside from matching requirements, there are other key factors to consider in ensuring an effective grant process, such as efficiency, timeliness, and oversight. For example, the DHS Office of Inspector General reported in March 2010 that DHS has a variety of preparedness grant programs with similar purposes, redundant application processes, and differing program requirements.[16] In our June 2009 report on the Transit Security Grant Program (TSGP), we identified problems with grant management and made recommendations related to defining agency roles when more than one agency is involved in the grant program, developing a plan for measuring effectiveness, developing a process to systematically collect data and track grant activities, and communicating the availability of grant funding to transit agencies.[17] Lacking these grant management characteristics, the TSGP experienced delays in approving projects and making funds available. As a result, about $21 million of the $755 million in awarded funds for fiscal years 2006 through 2008 had been expended by transit agencies. At the request of Ranking Member Peter T. King of the House Committee on Homeland Security, and Senator George V. Voinovich of the Senate Committee on Homeland Security and Governmental Affairs, this month we are initiating a review of grant management processes of selected DHS preparedness grant programs.

---

[15] GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).
[16] Department of Homeland Security, Office of Inspector General, *Efficacy of DHS Grant Programs*, OIG-10-69 (Washington, D.C., Mar. 22, 2010).
[17] GAO, *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO-09-491 (Washington, D.C.: June 8, 2009).

Question from Senator Hutchison

8. Various ports across the nation have indicated that the port security grant process is confusing, and that the distribution of funds is very slow, with FEMA and the USCG still working on delivering funds from 2007. What insights can GAO offer for a better, and more efficient, way to distribute port security grants, so that our nation's ports receive funds in a timely manner? GAO has made a number of recommendations to TSA and FEMA to improve the grant process for rail and transit security grants. Do any of those recommendations apply to port security grants? Is the Fiduciary Agent process an effective way to distribute port security grant funds?

While we have not reviewed issues related to the distribution of funding under the PSGP since 2005, and thus cannot offer solutions to current PSGP problems, we reported in our June 2009 report on the TSGP that defining agency roles, tracking grant activity, and distributing funds in a timely manner are important principles of grant management.[18] For example, given that the Federal Emergency Management Agency (FEMA) and Transportation Security Agency (TSA) share responsibility for the TSGP, we recommended that the two agencies define their respective roles and responsibilities for managing the TSGP. Similarly, FEMA and the Coast Guard should define their respective roles and responsibilities for managing the PSGP. We also reported that the systematic collection and tracking of grant activities under the TSGP is essential to effective grant management. At FEMA, the Grants Program Directorate (GPD)—which also oversees the PSGP—is responsible for this record keeping. However, GPD officials reported in March 2010 that the development of an updated grant management system—scheduled for completion in 2011—had been halted because of budget cuts. Lastly, because of delays that transit agencies experienced in receiving funding, we recommended that TSGP grant management officials establish time frames for making funds available to stakeholders that have had projects approved. Establishing such time frames could help grantees implement projects within the designated performance periods of the grants.

In addition to negotiating, tracking, and distributing funds, the process must also include key internal controls. In its *Guide to Opportunities for Improving Grant Accountability*, the Domestic Working Group reported that internal controls are needed to ensure that funds are properly used and achieve intended results.[19] It cites four areas where internal controls are important: (1) preparing policies and procedures before issuing grants, (2) consolidating information systems to assist in managing grants, (3) providing grant management training to staff and grantees, and (4) coordinating programs with similar goals and purposes. Establishing effective internal controls may slow the distribution of grants, as these systems should be in place prior to the grant award. However, the Domestic Working Group reported that inadequate internal controls make it difficult for grant managers to determine whether funds are properly used.

[18] GAO-09-491.

[19] The Domestic Working Group, consisting of 19 federal, state, and local audit organizations, was formed to identify current and emerging challenges and explore opportunities for greater collaboration within the intergovernmental audit community. The group identified grant accountability as a concern and created a project team to address this concern. The results are presented in the following report: *Domestic Working Group Grant Accountability Project: Guide to Opportunities for Improving Grant Accountability* (Washington, D.C., October 2005).

In terms of using a fiduciary agent, until fiscal year 2009, TSGP grant funding was first processed through a state administrative agency (SAA). However, the DHS appropriations acts for fiscal years 2009 and 2010 required funding to be provided directly to transit agencies.[20] We expect to follow up with transit agencies to identify the impacts of this change and determine whether the removal of the fiduciary agent added any efficiencies to the grant process as part of our upcoming review of grant management processes of selected DHS preparedness grant programs, requested by Ranking Member Peter T. King of the House Committee on Homeland Security, and Senator George V. Voinovich of the Senate Committee on Homeland Security and Governmental Affairs.

Transportation Worker Identification Credential

Question from Senator Lautenberg

9. Over a million maritime workers have gone through background checks and obtained TWIC cards, to gain access to secure areas of our ports. The Port Authority of New York/New Jersey is one of the sites testing these TWIC cards. However, this technology has been fraught with challenges and has not been working as intended. How do the challenges with the TWIC program affect the security of our ports?

In November 2009, we identified several Transportation Worker Identification Credential (TWIC) program challenges.[21] As noted in the report, the TWIC pilot is currently under way to test the use of TWIC cards with biometric card readers. Specifically, this pilot is intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. As such, the pilot is expected to test the viability of selected biometric card readers for use in reading TWIC cards within the maritime environment. It is also to test the technical aspects of connecting TWIC readers to access control systems. After the pilot has concluded, the results of the pilot are expected to inform the development of the card reader rule requiring the deployment of TWIC readers for use in controlling unescorted access to the secure areas of Maritime Transportation Security Act of 2002 (MTSA)—regulated vessels and facilities.[22] However, as noted in our November 2009 report, shortfalls in TWIC pilot planning have hindered the TSA and the Coast Guard's efforts to ensure that the pilot is broadly representative of deployment conditions and will yield the information needed—such as information on the operational impacts of deploying biometric card readers and their costs—to accurately inform Congress and the card reader rule. For instance, because of schedule constraints, TSA did not conduct its more rigorous laboratory testing of readers to be used at pilot sites prior to testing them at pilot sites as initially planned.

[20] Pub. L No. 110-329, 122 Stat. 3574, 3671 (2008); Pub. L. No. 111-83, 123 Stat. 2142, 2159 (2009).
[21] 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).
[22] Pub. L. No. 107-295, 116 Stat. 2064.

Since we issued our report in November 2009, TSA has received the results of the more rigorous laboratory-based reader durability testing. However, TSA has not shared the information on reader results with pilot participants. According to representatives of four of the seven pilot participants we met with, not sharing the results of reader testing has limited their ability to acquire the equipment that meets the environmental and durability needs of their port facilities and vessels and has resulted in their expending important port security funds without any assurance that their investment will be fruitful. Further, not all the approaches proposed in the Advanced Notice of Proposed Rule Making for using TWIC cards with readers will utilize the electronic security features on the TWIC card to confirm that the TWIC card is valid and authentic.

We are currently conducting a review of the TWIC program's internal controls related to enrollment, background checks, card production, card activation and issuance, and use. The results of this work, including related covert testing at port facilities, will be published in February 2011.

Question from Senator Nelson

10. Mr. Caldwell, does TSA share the information it gathers in its background investigations for Transportation Worker Identification Cards with state law enforcement entities?

TSA reports that it does not share the information that it gathers during the background investigations of TWIC applicants with state and local law enforcement entities on a routine basis. Pursuant to MTSA provisions restricting the use of applicant information and the TWIC Privacy Impact Assessment, TSA and the Coast Guard limit their sharing of information on applicants and card holders. MTSA also provides, however, that such information may be shared with other federal law enforcement agencies. According to TSA officials, on a case-by-case basis, TSA can decide to share information if TSA determines that there is an imminent threat (terrorist or criminal) of loss of life or property. According to TSA officials, in such a situation, TSA would provide only basic information, such as the type of threat, location, and individuals involved, but would likely not provide other information from a person's TWIC application. Additionally, state and local law enforcement entities may contact TSA if they identify criminal use of a TWIC card (e.g., a TWIC card used in commission of a crime, or presentation of a fraudulent TWIC card for entry into the secure area of a MTSA-regulated facility) or to verify the authenticity of a TWIC card.

Additionally, the Coast Guard and TSA have processes in place to share threat information with other federal law enforcement or terrorism centers. In the event that a TWIC applicant or TWIC cardholder is determined to pose a security threat, Coast Guard and TSA have developed a protocol to ensure effective interagency coordination and timely action to minimize the potential threat and risk to the maritime community associated with these individuals.

Supply Chain Security

Questions from Chairman Rockefeller

11. Has GAO's work made a formal determination of whether the 100 percent scanning requirement is consistent with risk management?

The application of risk management for container security can be considered at the strategic level (e.g., assessing risks to the entire supply chain and designing appropriate security programs) or the tactical level (e.g., assessing risks to individual containers and applying extra scrutiny through existing layered security programs). At the strategic level, federal law and presidential directives call for the use of risk management in homeland security as a way to protect the nation against possible terrorist attacks, and CBP uses risk management in its processes for mitigating potential threats posed by U.S.-bound cargo containers. Risk management generally calls for establishing risk management priorities and allocating limited resources to those assets that face the highest risk. Risk management is necessary in the context of container security because CBP, like other DHS components, cannot afford to protect all commerce against all possible threats. According to risk management frameworks developed by GAO and DHS, key phases of risk management should include (1) assessing the risk posed by terrorists' use of cargo containers and (2) evaluating alternative measures to counter that risk based on factors such as the degree of risk reduction they afford and the cost and difficulty to implement them.[23] This process includes a cost-benefit analysis of countermeasure options, which is useful in evaluating alternatives because it links the benefits from risk-reducing countermeasures to the costs associated with them. While we have not conducted an assessment of whether the 100 percent scanning requirement is consistent with risk management, our prior work indicates that 100 percent scanning is not consistent because this strategic analytic process did not occur. Specifically, our work has shown that DHS has not evaluated the cost-effectiveness of 100 percent scanning as a countermeasure as part of a risk management framework for cargo container security.[24]

At the tactical level, opponents of 100 percent scanning have taken the position that it is better to assess the risk posed by each container and apply a countermeasure that is tailored to that container—as opposed to assessing the risk posed to supply chain security by cargo containers in general and then determining the most cost-effective countermeasure to reduce that risk (e.g., 100 percent scanning, CBP's layered security approach, or another alternative). From this perspective, the 100 percent scanning requirement is a departure from existing CBP container security programs because it requires CBP to scan all containers before performing analysis to determine their potential risk level. This position applies risk management principles—establishing strategic goals and priorities and allocating limited resources to those assets that face

[23] GAO-06-91 and DHS, *National Infrastructure Protection Plan*, *Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).
[24] GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

the highest risk—at the individual container level. According to this view, the 100 percent scanning requirement is inconsistent with risk management principles because it does not distinguish among containers based on risk; rather, it assumes that all containers have an equal risk of carrying terrorist weapons and are to be subjected to the same level of scrutiny with the same amount of resources. Thus, resources are applied uniformly across all cargo containers rather than being allocated based on the potential risk they pose. Opponents of 100 percent scanning who have generally taken this position include CBP, foreign governments, and industry. For example, the former Acting Commissioner and current Commissioner of CBP have said that the 100 percent scanning requirement is not a risk-based approach. Similarly, foreign governments have expressed the view that 100 percent scanning is not consistent with risk management principles as contained in the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework). For example, European and Asian customs officials told us that the 100 percent scanning requirement is in contrast to the risk-based strategy, that serves as the basis for other U.S. programs, such as the Container Security Initiative (CSI)[25] and the Customs-Trade Partnership Against Terrorism (C-TPAT).[26] The WCO, representing customs agencies around the world, stated that the implementation of 100 percent scanning would be "tantamount to abandonment of risk management." In terms of industry, in 2008 the Association of German Seaport Operators released a position paper that stated that implementing the 100 percent scanning requirement would undermine mutual, already achieved security successes and deprive resources from areas that present a more significant threat and warrant closer scrutiny. Closer to home, the Commercial Operations Advisory Committee—an official industry group to CBP—has recently called for the repeal of the 100 percent scanning requirement and a move toward a more risk-based approach.[27]

Still at the tactical level, supporters of 100 percent scanning have expressed concerns about the effectiveness of existing CBP programs that attempt to assess the risks of individual containers and subject those deemed higher risk to closer scrutiny, including non-intrusive inspection (NII) scanning. Members of Congress who spoke in favor of the 100 percent scanning requirement noted that scanning all containers overseas could help detect weapons of mass destruction concealed in containers that are not identified as high risk because of weaknesses in CBP's layered security strategy. That is, 100 percent scanning would be a more effective way to counter the risks posed to cargo containers than existing initiatives intended to identify high-risk containers. In making these arguments, certain members of Congress also cited GAO work that had identified potential weaknesses in programs that make up the layered security strategy. Our work identified weaknesses including a lack of validation of CBP's targeting practices through strategies like red-teaming; inadequate validation of C-TPAT members' security practices prior to granting them program benefits, such as a decreased likelihood of having their

[25] CBP places staff at participating foreign ports to work 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.

[26] Through the C-TPAT program, CBP develops voluntary partnerships with members of the international trade community comprised of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies agree to improve the security of their supply chains in return for various benefits, such as reduced examination of their cargo.

[27] The Commercial Operations Advisory Committee advises the Secretaries of the Treasury and Homeland Security on the commercial operations of CBP and related DHS and Department of the Treasury functions.

shipments scanned or physically examined; and not ensuring that containers identified as high risk but not scanned at CSI ports overseas are scanned upon arrival in the United States.[28] The concerns we raised were open issues at the time Congress considered the 100 percent scanning requirement; however, since that time, these CBP programs have matured, and many of our recommendations have been implemented.[29]

As mentioned above, risk management includes not just assessing risks, but also evaluating alternative measures based on such factors as the degree of risk reduction they afford and the cost and difficulty to implement them. Our work has documented that there are operational challenges—such as logistics, technology, and infrastructure—to implementing 100 percent scanning.[30] However, CBP has not done a detailed analysis to determine the feasibility of 100 percent scanning within the context of its risk-based layered security strategy. In this case, part of evaluating alternative measures is determining a concept of operations—a description of the operations that must be performed, who must perform them, and where and how the operations will be carried out—for how 100 percent scanning would work at foreign ports, which would include conducting studies and analyses at each port to determine locations where NII equipment would be able to scan 100 percent of containers going to the United States with a minimum of disruption to the flow of commerce at the port. For instance, transshipment—cargo containers from one port that are taken off a vessel at another port to be placed on another vessel bound for the United States—poses a particular challenge to 100 percent scanning. According to European customs officials, implementing the 100 percent scanning requirement at large ports with complex operations would likely result in the need for a fundamental redesign of several ports, entailing substantial costs to terminal users. For other scanning options, the costs may not be as great. For example, as we describe in more detail in the next section, scanning with only radiation portal monitors (RPM) is less costly in terms of both equipment and impact on the flow of commerce.

No homeland security program can guarantee complete success or freedom from risk, and CBP officials have acknowledged that they will likely not be able to achieve 100 percent scanning of U.S.-bound cargo containers by the statutory deadline.[31] However, we believe additional analysis, done within a risk management framework, can help improve container security. In our October 2009 report on the Secure Freight Initiative (SFI) and 100 percent scanning, we recommended that among other things, CBP perform feasibility and cost-benefit analyses to (1) better position itself to determine the most effective way forward to enhance container security, (2) improve its container security

---

[28] See for example, GAO, C*argo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 11, 2005), and *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004).

[29] We previously reported on the maturing of these programs and the implementation of our recommendations in GAO, *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2007).

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

[31] The statute provides that containers loaded at foreign ports on or after July 1, 2012 shall not enter the United States unless they were scanned by NII equipment and radiation detection equipment prior to loading. It also provides for renewable, two-year extensions if DHS certifies to Congress that certain conditions exist at a port or ports, such as equipment not being available for purchase and installation, physical constraints, or a significant impact on trade capacity and flow of cargo. See 6 U.S.C. § 982(b).

programs, and (3) better inform Congress. DHS agreed in part with our recommendation that it develop a cost-benefit analysis of 100 percent scanning, acknowledging that the recommended analyses would better inform Congress, but stated that the recommendation should be directed to the Congressional Budget Office. While the Congressional Budget Office does prepare cost estimates for pending legislation, we think the recommendation is appropriately directed to CBP. Given its daily interaction with foreign customs services and its direct knowledge of port operations, CBP is in a better position to conduct any cost-benefit analysis and bring results to Congress for consideration. We believe that such analyses could help to guide DHS, CBP, and Congress in their efforts to either implement the 100 percent scanning requirement or assess other approaches to enhancing container security.

12. S. 3639 makes a technical amendment so that all U.S.-bound containers be scanned with either RPM or NII, but not both. It also extends the deadline for the requirement by three years from 2012 to 2015. What are the advantages of this approach to 100 percent scanning?

Based on our review of the 100 percent scanning requirement, scanning containers with RPMs instead of in combination with NII equipment may be more achievable from a technology, logistics, political, and cost standpoint.[32] However, there are limitations to relying solely on RPMs for scanning cargo containers that should be taken into consideration.

- **Technology/logistics**: Scanning containers with RPM equipment is generally less time-consuming than scanning with NII equipment. While the actual NII scanning time per container can take as little as 20 seconds, depending on the system, the entire inspection time can take longer than 6 minutes. As part of the scanning process, customs officers need time to (1) stage the container to align it properly between the system's radiation source and detector array, (2) verify the container information with the manifest, (3) ensure that the system is set to receive scanned images, (4) interpret the scanned images and verify them using manifest information, (5) identify and document any anomalies, (6) save the scanned images, (7) check the integrity of the seal and verify the seal number, and (8) prepare the system for the next container. While scanning cargo containers with NII equipment involves several steps, in contrast it takes the driver of a standard tractor trailer from 4 to 7 seconds to pass through a RPM.[33]

- **Political:** Although 173 members of the WCO expressed their opposition to the 100 percent scanning requirement, in a letter to members of Congress in September 2008, the WCO noted that it did not object to the requirement that all cargo containers be subjected to radiation detection processes (i.e., RPM scanning) prior to shipment to the United States. In addition, foreign government officials we spoke with stated that they are generally not opposed to the use of radiation detection equipment—such as

[32] GAO-10-12.

[33] Containers that trigger a radiation alarm at the RPM undergo a second exam with a handheld radiation detection device to help ensure that the source of the alarm is identified and resolved. The exam with the handheld radiation detection device typically requires 5 to 10 minutes to perform.

the RPMs that are used as part of the Megaports Initiative[34]—but they are opposed to the use of NII equipment because of the likelihood that it may hinder trade and reduce security by consuming a large amount of scarce resources (i.e., key dock space and increased time needed for cargo container inspections) for comparatively little benefit.

- **Cost:** RPM equipment is less expensive than NII equipment. The price for polyvinyl toluene monitors—the type of RPMs most commonly used at U.S. seaports—is $425,000 per unit (including deployment costs). In contrast, the purchase price for large-scale NII systems used by CBP at U.S. seaports is approximately $3 million per system (including deployment costs).

- **Limitations of RPMs:** Scanning containers with RPMs alone introduces the vulnerability of not detecting shielded nuclear material. However, if customs officials believe based on targeting data that further inspections are necessary, they can have a container scanned by NII equipment.

In addition to the factors listed above, the Department of Energy's National Nuclear Security Administration (NNSA) has a goal through the Megaports Initiative of scanning as much global cargo container traffic as possible with RPMs. Since the start of the Megaports Initiative in fiscal year 2003, NNSA has completed installations of RPM equipment at 27 foreign ports, and implementation is under way at an additional 16 foreign ports. The Megaports Initiative seeks to equip 100 ports with radiation detection systems by 2015, scanning approximately 50 percent of global maritime containerized cargo.

13. DHS and CBP have cited the Strategic Trade Corridor and the Importer Security Filing (10+2) as alternative ways to enhance supply chain security. They have also stated that new technology for containers themselves, and the equipment used to scan them, is another path forward to improve supply chain security. What work does GAO have on these programs and what is the status of these DHS efforts?

Strategic Trade Corridor Strategy

The Secretary of Homeland Security has endorsed the concept of a strategic trade corridor strategy as the path forward for implementing the SFI program, but DHS and CBP have not yet selected the ports or funded the expansion of SFI. In particular, in April 2009, the Secretary of Homeland Security was presented with three options for implementing the SFI program, ranging from implementing SFI at 70 ports that account for shipping over 90 percent of U.S.-bound containers to seeking repeal of the 100 percent scanning requirement. The strategic trade corridor strategy option selected by the Secretary focuses cargo container scanning efforts on a limited number of ports where CBP has determined that SFI will help mitigate the greatest risk of potential weapons of mass destruction entering the United States. According to CBP's report,

[34] Through the Megaports Initiative, the Department of Energy installs radiation detection equipment at key foreign ports, enabling foreign government personnel to use radiation detection equipment to scan shipping containers entering and leaving these ports, regardless of the containers' destination, for nuclear and other radioactive material that could be used against the United States and its allies.

Risk-Based, Layered Approach to Supply Chain Security, sent to Congress in April 2010, the data gathered from SFI operations will help to inform future deployments to strategic locations.[35] The report further added that CBP plans to evaluate the usefulness of these deployments and consider whether the continuation of scanning operations adds value in each of these locations and in potential additional locations that would strategically enhance CBP efforts. However, in DHS's *Congressional Budget Justification for FY 2011*, CBP requested a decrease in the SFI program's $19.9 million budget by $16.6 million and did not request any funds to implement the strategic trade corridor strategy. According to the budget justification, in fiscal year 2011, SFI operations will be discontinued at three SFI ports—Puerto Cortes, Honduras; Southampton, United Kingdom; and Busan, South Korea—and the SFI program is to be established at the Port of Karachi, Pakistan. We issued a report in October 2009 that provides further details about the implementation of the SFI program.[36]

Importer Security Filing Program

While CBP has implemented the Importer Security Filing and Additional Carrier Requirements,[37] collectively known as the 10+2 rule, and is using the information to identify high-risk unmanifested containers, CBP has not yet fully incorporated the collected data into its targeting process. In January 2009, CBP implemented the 10+2 rule, which mandates that importers and vessel carriers submit additional cargo information, such as country of origin, to CBP before the cargo is loaded onto a U.S.-bound vessel.[38] Collection of the additional cargo information (10 data elements for importers and 2 data elements for vessel carriers) and their incorporation into CBP's Automated Targeting System (ATS)[39] are intended to enhance CBP's ability to identify high-risk shipments and prevent the transportation of potential terrorist weapons into the United States via cargo containers. CBP has assessed the submitted 10+2 data elements for risk factors, and according to CBP officials, access to information on stow plans[40] has enabled CBP to identify more than 1,000 unmanifested containers—containers that are inherently high risk because their contents are not listed on a ship's manifest. However, although CBP has conducted a preliminary analysis that indicates that the collection of the additional 10+2 data elements could help determine risk earlier in the supply chain, CBP has not yet finalized its national security targeting weight set for identifying high-risk cargo containers or established project time frames and milestones—best practices in project management—for doing so. We recommended that CBP establish milestones and time frames for updating its national security weight set to use 10+2 data in its identification of shipments that could pose a threat to national security. DHS concurred with this recommendation and said it plans to complete its

[35] U.S. Customs and Border Protection, *Risk-Based, Layered Approach Supply Chain Security, Fiscal Year 2010 Report to Congress* (Washington D.C., Apr. 13, 2010).
[36] GAO-10-12.
[37] Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (to be codified at 19 C.F.R. pts. 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, and 192).
[38] Under other requirements that preceded the 10+2 rule, importers are also required to provide customs entry information, and carriers are required to provide cargo manifest information under the 24-hour rule.
[39] ATS is a computer model that CBP uses to analyze shipment data for risk factors and target potentially high-risk oceangoing cargo containers for inspection. For more information on ATS, see GAO, *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*, GAO-06-591T (Washington, D.C.: Mar. 30, 2006), and GAO-04-557T.
[40] Stow plans depict the position of each cargo container on a vessel.

updates to the national security weight set by November 2010. More information on the results of our review can be found in our September 2010 report.[41]

Container Security Technologies

DHS is testing and evaluating technologies for detecting and reporting intrusions into and tracking the location of cargo containers as they pass through the global supply chain, but it will take time before the evaluations are complete and the technology and implementation challenges are overcome for some of these technologies. In particular, CBP has partnered with DHS's Science and Technology Directorate (S&T) to develop performance standards—requirements that must be met by products to ensure that they will function as intended—for four container security technologies with the goal of having the ability to detect and report intrusion into, and track the movement of cargo containers through the global supply chain. If S&T is able to demonstrate through testing and evaluation that container security technologies exist that can meet CBP's requirements, then it plans to provide performance standards to CBP and DHS's Office of Policy Development to pursue for implementation. From 2004 through 2009, S&T spent over $60 million and made varying levels of progress on its four container security technology projects. Each of these projects has undergone laboratory testing, but S&T has not yet conducted operational environment testing to ensure that the prototypes will satisfy the requirements so that S&T can provide performance standards to the Office of Policy Development and CBP. Performance standards are expected to be completed for two of the technologies by the end of 2010, but it could take time before they are complete for the other two technologies. More information on the results of our review of container security technologies may be found in our September 2010 report.[42]

Cargo Advanced Automated Radiography System

We also reviewed DHS efforts to improve NII scanning through the cargo advanced automated radiography system (CAARS) program. DHS intended for CAARS to be used by CBP to automatically detect and identify highly shielded nuclear material in vehicles and cargo containers at U.S. ports of entry. However, DHS's Domestic Nuclear Detection Office (DNDO) pursued the acquisition and deployment of CAARS machines without fully understanding that they would not fit within existing primary inspection lanes at CBP ports of entry. This occurred because during the first year or more of the program DNDO and CBP had few discussions about operating requirements at ports of entry. Further, the development of the CAARS algorithms (software)—a key part of the machine needed to identify shielded nuclear materials automatically—did not mature at a rapid enough pace to warrant acquisition and deployment. These factors contributed to DNDO's December 2007 decision to make a "course correction" in the program resulting in cancellation of the acquisition and deployment plans for CAARS. Through this action, DNDO significantly reduced the scope of CAARS to a research and development effort designed to demonstrate the potential capability of the technology. While the development of CAARS-type or other advanced radiography equipment capable of

[41] 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).
[42] GAO, *Supply Chain Security: DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended*, GAO-10-877 (Washington, D.C.: Sept. 29, 2010).

automatic detection of highly shielded nuclear material in cargo containers has been ongoing since 2005, one senior CBP official acknowledged that it is not known when the technology will be sufficiently mature for agencies within DHS, such as CBP, to justify acquiring and deploying it in large numbers. On September 30, 2010, the Director of DNDO announced that DNDO is terminating the CAARS program. However, the technology developed under the CAARS program may be utilized by other programs. More information on the results of our review of CAARS may be found in our September 2010 statement for the record for the Senate Committee on Homeland Security and Governmental Affairs.[43]

[43] GAO, *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials*, GAO-10-1041T (Washington, D.C.: Sept. 15, 2010).

Enclosure 2

GAO Contact and Staff Acknowledgments

GAO Contact
Stephen L. Caldwell, (202) 512-9610, or caldwells@gao.gov

Staff Acknowledgments
In addition to the contact named above, Dawn Hoff, Assistant Director; Jonathan Bachman; Chuck Bausell; Lisa Canini; Christopher Conrad; Frances Cook; Tracey Cross; Alana Finley; Geoff Hamilton; Christine Hanson; Mike Harmond; Christopher Hatscher; Dawn Hoff; Richard Hung; Tracey King; Daniel Klabunde; Lara Miklozek; Julie Silvers; and Katy Trenholme were key contributors to this letter.

(440924)