United States Government Accountability Office

GAO

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, February 7, 2012

SUPPLY CHAIN SECURITY

Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning

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

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-422T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

February 7, 2012

SUPPLY CHAIN SECURITY

Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning

Why GAO Did This Study

Cargo containers that are part of the global supply chain—the flow of goods from manufacturers to retailers–are vulnerable to threats from terrorists. The Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability For Every (SAFE) Port Act of 2006 required the Department of Homeland Security (DHS) to take actions to improve maritime transportation security. Also, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) required, among other things, that by July 2012, 100 percent of all U.S.-bound cargo containers be scanned. Within DHS, U.S. Customs and Border Protection (CBP) is responsible for container security programs to address these requirements. This testimony addresses, among other things, (1) efforts to gather advance information about container shipments to assess risks, (2) technologies used to protect the integrity of containers and scan them, and (3) the status of efforts to scan 100 percent of U.S.-bound containers. GAO's statement is based on products issued from April 2005 through July 2011, along with selected updates conducted from January to February 2012. Updates involved collecting information from CBP on the status of efforts to address GAO's prior recommendations on these issues and its plans to implement 100 percent scanning.

What GAO Recommends

GAO has made recommendations in past reports to DHS to strengthen its container security efforts. DHS concurred with GAO's recommendations and has either addressed them or is undertaking efforts to address them.

View GAO-12-422T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

As part of its efforts to identify high-risk cargo for inspection, CBP uses various sources of information to screen containers in advance of their arrival in the United States. For example, in 2009, CBP implemented the Importer Security Filing and Additional Carrier Requirements to collect additional information for targeting. The additional cargo information required, such as country of origin, is to be provided to CBP in advance of arrival of the cargo containers at U.S. ports. In September 2010, GAO recommended that CBP establish milestones and time frames for updating its targeting criteria to include additional information. In response, CBP updated its targeting criteria in January 2011.

DHS has made some progress in developing and implementing container security technologies to protect the integrity of containers and to scan them. GAO reported in September 2010 that DHS's Science and Technology Directorate initiated four container security technology projects to detect and report intrusions into cargo containers. However, operational testing had not occurred to ensure the prototypes would function as intended. Therefore, GAO recommended that testing and evaluation occur in all environments in which DHS planned to implement the technologies. DHS concurred and has made progress implementing this recommendation. To prevent the smuggling of nuclear and radiological materials, CBP, in coordination with the Domestic Nuclear Detection Office (DNDO), has deployed over 1,400 radiation portal monitors (RPM) at U.S. ports of entry to detect the presence of radiation in cargo containers. Since 2006, GAO reported on problems with DNDO's efforts to deploy a more-advanced and significantly more-expensive type of RPM. Among other things, GAO reported that an updated cost-benefit analysis might show that DNDO's program to replace existing equipment with the advanced technology was not justified. After spending more than $200 million, DHS ended the program in July 2011.

Uncertainty persists over how DHS and CBP will fulfill the mandate for 100 percent scanning given that the feasibility remains unproven in light of the challenges CBP has faced implementing a pilot program for 100 percent scanning. In response to the SAFE Port Act requirement to implement a pilot program to determine the feasibility of 100 percent scanning, CBP, the Department of State, and the Department of Energy announced the formation of the Secure Freight Initiative (SFI) pilot program in December 2006. However, logistical, technological, and other challenges prevented the participating ports from achieving 100 percent scanning and CBP has since reduced the scope of the SFI program from six ports to one. In October 2009, GAO recommended that CBP perform an assessment to determine if 100 percent scanning is feasible, and if it is, the best way to achieve it, or if it is not feasible, present acceptable alternatives. However, to date, CBP has not conducted such an assessment or identified alternatives to 100 percent scanning. Further, as GAO previously reported, DHS acknowledged it will not be able to meet the 9/11 Act's July 2012 deadline for implementing the 100 percent scanning requirement, and therefore, it expects to grant a blanket extension to all foreign ports pursuant to the statute, thus extending the target date to July 2014. To do so, DHS is required to report to Congress by May 2, 2012, of any extensions it plans to grant.

Chairman Miller, Ranking Member Cuellar, and Members of the Subcommittee:

I am pleased to be here today to discuss the status of federal efforts to enhance the security of maritime cargo containers used for shipping many imports to the United States. The potential for terrorists to smuggle weapons of mass destruction (WMD) inside cargo containers bound for the United States has remained a concern since the terrorist attacks of September 11, 2001. Cargo containers are an important segment of the global supply chain—the flow of goods from manufacturers to retailers. In 2011, about 10.7 million oceanborne cargo containers arrived at U.S. ports, and according to the U.S. Department of Transportation, the majority of U.S. imports arrive by ocean vessel.[1] The typical supply chain process for transporting cargo containers to the United States involves many steps and participants. For example, the cargo containers, and the goods in them, can be compromised not only by the manufacturers or suppliers of the goods being shipped, but also by vessel carriers who are responsible for transporting the containers from foreign ports to U.S. ports, as well as by personnel who load and unload cargo containers onto and off vessels.[2]

Given the complexity of the global supply chain process and the vast number of cargo containers that are shipped to the United States each year, the global supply chain is vulnerable to threats that terrorists and criminals might be able to exploit. As we reported in October 2009, while the Department of Homeland Security (DHS) has noted that the likelihood of terrorists smuggling WMD into the United States in cargo containers is low, the nation's vulnerability to this activity and the consequences of such an attack—such as billions of losses in U.S revenue and halts in manufacturing production—are potentially high.[3]

[1] U. S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, A*merica's Container Ports: Linking Markets at Home and Abroad* (Washington, D.C.: January 2011).

[2] Cargo containers serve, in essence, as packing crates and portable warehouses for virtually every type of general cargo moving in the supply chain.

[3] In 2002, the consulting firm Booz Allen Hamilton sponsored a simulated scenario in which the detonation of weapons smuggled in cargo containers shut down all U.S. seaports for 12 days—resulting in a loss of $58 billion in revenue to the U.S. economy along with significant disruptions to the movement of goods.

November of 2012 will mark the 10th anniversary of the enactment of the Maritime Transportation Security Act (MTSA) of 2002,[4] which, among other things, called for the establishment of a program to evaluate and certify secure systems of international intermodal transportation, including standards and procedures for screening and evaluating cargo prior to loading and for securing and monitoring cargo while in transit.[5] In 2006, the Security and Accountability For Every (SAFE) Port Act,[6] which amended MTSA, required DHS to develop, implement, and update as appropriate a strategic plan to enhance the security of the international supply chain.[7] To address concerns regarding international supply chain security, U.S. Customs and Border Protection (CBP), a component of DHS, developed a layered security strategy for cargo containers. Core components of the layered security strategy include analyzing information to identify containers that may be at high risk of transporting WMD or other contraband, working with governments of other nations to examine containers CBP has determined to be high risk before such containers are loaded onto U.S.-bound vessels at foreign ports, and providing benefits to companies that comply with predetermined security measures.

The SAFE Port Act further requires that pilot projects be established at three ports to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.[8] In August 2007, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) was enacted,[9] which requires, among other things, that by July 2012, 100 percent of all U.S.-bound cargo containers be scanned at foreign ports with both radiation-detection and nonintrusive inspection equipment

[4] Pub. L. No. 107-295, 116 Stat. 2064.

[5] See 46 U.S.C. § 70116.

[6] Pub. L. No. 109-347, 120 Stat. 1884.

[7] The SAFE Port Act required DHS to report to Congress on this strategic plan by July 2007, with an update of the strategic plan to be submitted to Congress 3 years later. See 6 U.S.C. § 941(a), (g).

[8] 6 U.S.C. § 981. A similar requirement was enacted that same year by the Department of Homeland Security Appropriations Act, 2007 (Pub. L. No. 109-295, 120 Stat. 1355 (2006)) and is codified at 6 U.S.C. § 981a. Both statutes specify scanning as examination with both radiation detection equipment and nonintrusive imaging equipment. 6 U.S.C. §§ 981(a), 981a(a)(1).

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

before being placed on U.S.-bound vessels,[10] with possible extensions for ports at which certain conditions exist.[11] Further, in July 2007, DHS issued the strategic plan called for in the SAFE Port Act, entitled the *Strategy to Enhance International Supply Chain Security*,[12] and on January 23, 2012, the administration issued the *National Strategy for Global Supply Chain Security*,[13] which describes a strategy for promoting the efficient and secure movement of goods and fostering a resilient supply chain.

DHS and CBP have taken various actions to enhance maritime container security. As requested, this statement addresses our work in this area and includes the following topics:

- efforts to gather advance information about container shipments to assess the risks of these containers,
- technologies used to protect the integrity of containers and to scan them to detect WMD and other contraband,
- partnerships with foreign governments and the private sector to improve container security efforts, and
- the status of efforts to scan 100 percent of U.S.-bound cargo containers.

This statement is based on related GAO reports and testimonies issued from April 2005 through July 2011, which addressed various programs that constitute CBP's layered security strategy, along with selected

[10] Radiation-detection equipment identifies radiation being emitted from a container, and through nonintrusive inspection CBP can identify anomalies in a container's image which could, among other things, indicate the presence of shielding material.

[11] The 9/11 Act scanning provision includes possible extensions for a port or ports for which DHS certifies that at least two out of a list of specific conditions exist. Among others, these conditions include (1) adequate scanning equipment is not available or cannot be integrated with existing systems, (2) a port does not have the physical characteristics to install the equipment, or (3) use of the equipment will significantly impact trade capacity and the flow of cargo. *See* 6 U.S.C. § 982(b)(4).

[12] DHS, *Strategy to Enhance International Supply Chain Security* (Washington, D.C.: July 2007).

[13] The White House, *National Strategy for Global Supply Chain Security* (Washington, D.C.: Jan. 23, 2012).

updates conducted from January 2012 to February 2012.[14] For our prior reports and testimonies, among other things, we analyzed CBP documents; reviewed legal documentation; and interviewed foreign government, DHS, CBP, and trade industry officials. We also conducted site visits to select ports that participate in CBP's container security programs and CBP's National Targeting Center – Cargo.[15] Additional details on the scope and methodology for those reviews are available in our published products. For the updates, we collected information from CBP on actions it has taken to address recommendations made in prior GAO reports on which this statement is based. We also reviewed publicly available documents, such as CBP's budget justifications for fiscal years 2011 and 2012 and the administration's National Strategy for Global Supply Chain Security, for information regarding DHS's and CBP's plans for implementing the 100 percent scanning requirement. We conducted this work in accordance with generally accepted government auditing standards.

CBP Has Various Tools for Targeting U.S.-Bound Cargo Containers for Inspections

As part of its efforts to target high-risk cargo containers for inspection, CBP uses various sources of information to screen containers in advance of their arrival in the United States. Specifically, CBP's 24-hour rule requires that vessel carriers submit cargo manifest information to CBP 24 hours before U.S.-bound cargo is loaded onto a vessel. To further enhance CBP's ability to target high-risk shipments, in 2006 the SAFE Port Act required CBP to collect additional data related to the movement of cargo to identify high-risk cargo for inspection,[16] and in 2009 CBP implemented the Importer Security Filing and Additional Carrier Requirements, collectively known as the 10+2 rule.[17] The cargo information required by the 10+2 rule comprises 10 data elements from importers, such as country of origin, and 2 data elements from vessel carriers, such as the position of each container transported on a vessel, all of which are to be provided to CBP in advance of arrival at a U.S. port.

[14] See the list of GAO's related products included at the end of this statement.

[15] The National Targeting Center – Cargo is responsible for targeting high-risk shipments for inspection.

[16] *See* 6 U.S.C. § 943(b).

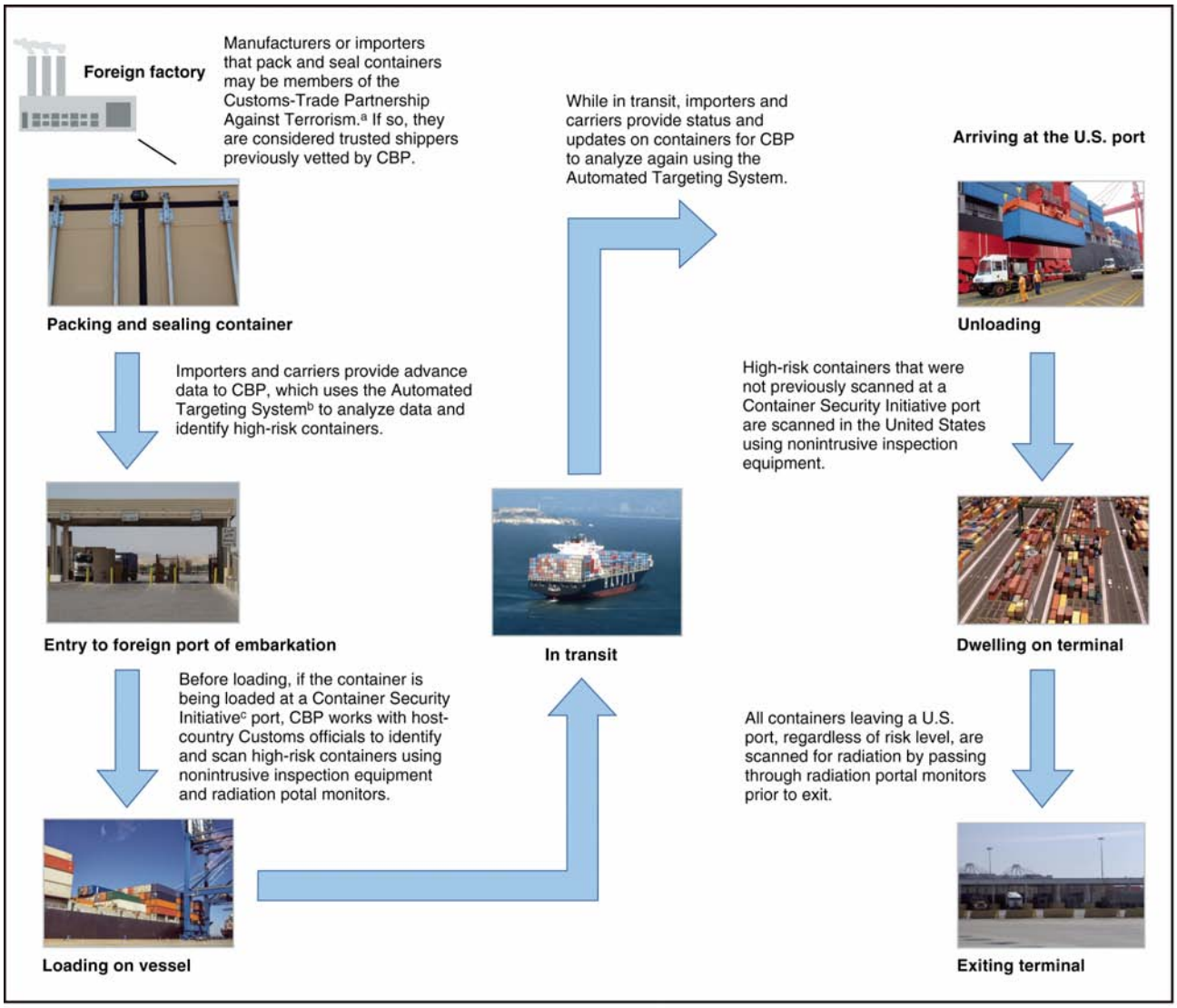
[17] Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (codified at 19 C.F.R. pts. 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, & 192).

Some of the data are required to be submitted prior to loading the container onto a U.S.-bound vessel.[18] Additionally, the United States has worked to expand the program beyond domestic implementation by coordinating with the World Customs Organization (WCO)[19] to incorporate some of the 10+2 data elements into the international supply chain security standards, which are discussed later in this statement. (Fig. 1 illustrates where CBP's container security programs intersect with the key points of transfer in the global supply chain.)

[18] 19 C.F.R. §§ 4.7c, 149.3(a)-(b).

[19] The WCO is an independent international organization whose mission is to enhance the efficiency and effectiveness of customs administrations.

Figure 1: Global-Supply Chain Process



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

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

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

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

Data that CBP collects on U.S.-bound cargo containers and their contents are fed into the Automated Targeting System (ATS)—a computerized model that CBP uses as a decision-support tool in targeting cargo containers for inspection.[20] Specifically, within ATS, CBP uses various data elements to determine an overall risk score for a particular threat in a shipment. CBP officers use these scores to help them make decisions on the extent to which documentary reviews or nonintrusive inspections are to be conducted on cargo containers. In our September 2010 report on the implementation of the 10+2 rule, we recommended that CBP establish milestones and time frames for updating ATS to use the 10+2 data in its identification of shipments that could pose a threat to national security. In response to this recommendation, CBP took steps in January 2011 to improve targeting efforts by updating its targeting criteria in to include risk factors present in the 10+2 data.[21] We recently began a review of the effectiveness of ATS as part of CBP's targeting efforts and plan to issue a report later this year.[22]

[20] 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).

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

[22] We are conducting this work for the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives.

DHS Has Made Some Progress in Implementing Technologies to Improve Container Security

Container Security Technologies Are Intended to Detect Intrusion and Track Movement

As we reported in September 2010, DHS's Science and Technology Directorate (S&T) initiated four container security technology projects,[23] in part, in response to general MTSA requirements,[24] as well as CBP's need for technologies to detect intrusion and track the movement of containers through the supply chain.[25] Specifically, a CBP study recognized that existing container seals provided inadequate security against physical intrusion (e.g., removing a container door to bypass a container seal) and therefore CBP should develop a technology to monitor and record intrusions on any of the six sides of a container. In September 2010, we reported that DHS had conducted research and development for these projects, but had not yet developed performance standards for them. Specifically, each project had undergone laboratory testing, but S&T had not yet conducted testing in an operational environment to ensure that the prototypes for those projects that had passed laboratory testing would function as intended. Furthermore, S&T's plans for conducting operational testing, did not reflect all of the operational scenarios being considered for implementation. We recognized that successfully testing the performance of these technologies is a precursor to developing performance standards

[23] Two of the four container security technology projects were to detect intrusion on all six sides of a container; one of them was to detect intrusion on one side (i.e., the door); and, one of them was to track containers and communicate the intrusion to the appropriate officials.

[24] See 46 U.S.C. § 70116. (requiring a program that includes establishing standards and procedures for securing and monitoring cargo in transit, as well as performance standards to enhance the physical security of shipping containers, including standards for seals and locks).

[25] 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-10-887 (Washington, D.C.: Sept. 29, 2010).

for them; therefore, we recommended that DHS test and evaluate the technologies within all of the operational scenarios DHS identified for potential implementation before S&T provides performance standards to the Office of Policy Development and CBP—DHS concurred with our recommendation and has completed operational testing for two of the four container security technology projects in the maritime environment.[26] S&T officials considered the laboratory and operational testing of both technology projects a success because they were proven to function under one operational scenario, which resulted in the development of performance standards that are necessary to pursue implementation of these technologies. To fully address our recommendation, however, DHS would need to test and evaluate the technologies within each of the remaining operational scenarios it identified for potential implementation. DHS has informed us that it plans to conduct further operational testing and anticipates completing this testing in May 2013.

We also reported on the challenges DHS and CBP could face regarding the implementation of the four container security technology projects.[27] For example, DHS and CBP could face challenges in obtaining support from the trade industry and international partners as it pursues implementation of the security technologies. Specifically, some members of the trade industry we spoke with were resistant to purchasing and using the technologies given the number of container security programs with which they already have to comply. DHS will also need to obtain support from international organizations and the WCO to implement new container security technologies. For instance, for container security technologies to be admitted to foreign countries without being subject to import duties and taxes, as well as import prohibitions and restrictions, the technologies first have to be recognized as accessories and equipment of the containers under the Customs Convention on Containers.[28] The successful implementation of security technologies also depends on the security procedures throughout the supply chain as well

[26] Laboratory and operational testing has been completed for the project to detect intrusion through the door of the container and the project to track containers and communicate intrusions.

[27] GAO-10-887.

[28] The convention essentially provides for the temporary and admission and reexportation of containers and their accessories and equipment that meet certain requirements without imposition of duties or taxes by any customs authority.

as people engaged in those procedures, which are typically documented in the concept of operations. As a result, DHS and CBP could face challenges developing a feasible concept of operations that addresses the necessary technology infrastructure needs and protocols. Container security technologies require a supporting technology infrastructure, including readers to communicate to customs officials whether a technology has identified an intrusion. Thus, CBP will be faced with determining who will have access to the container security technologies through readers, where to place these readers, and obtaining permission to install fixed readers at domestic and foreign ports. Also, protocols will need to be developed to identify which supply chain participants will be involved in arming and disarming the technologies, reading the status messages generated by the technologies, responding to alarms, and accessing data.

Radiation Detection and Nonintrusive Imaging Technology Can Help Identify Container Contents

To prevent the smuggling of nuclear and radiological materials, as of September 2010, CBP in coordination with DHS's Domestic Nuclear Detection Office (DNDO), has deployed over 1,400 radiation portal monitors (RPM) at U.S. ports of entry. Most of the RPMs are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass before they can exit U.S. ports. These monitors alarm when they detect radiation. CBP then conducts further inspections of the suspect contents at its secondary inspection locations to identify the cause of the alarm and determine what further security measures, if any, need to be taken.

While these RPMs are sensitive and have been effective at detecting radiation, they also have limitations. In particular, in May 2009 we reported that RPMs are capable of detecting certain nuclear materials only when these materials are unshielded or lightly shielded.[29] In contrast, advanced nonintrusive inspection equipment can be used to detect dense material that may be consistent with the presence of certain nuclear materials. CBP already uses nonintrusive inspection equipment to more closely investigate the contents of cargo containers that it has selected for secondary inspection at a U.S. port of entry; however, according to CBP

[29] GAO, *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology*, GAO-09-655 (Washington, D.C.: May 21, 2009).

officials, only a small percentage of vehicles or cargo containers are subjected to secondary inspections.

Since 2006, we have been reporting on long-standing problems with DNDO's efforts to deploy advanced spectroscopic portal (ASP) radiation detection monitors, a more-advanced and significantly more-expensive type of RPM designed to replace the RPMs CBP currently uses. GAO last reported on ASP testing in 2009 and found that DHS's cost analysis of the ASP program did not provide a sound analytical basis for DHS's decision to deploy the portals.[30] We also reported that an updated cost-benefit analysis might show that DNDO's plan to replace existing equipment with ASPs was not justified, particularly given the marginal improvement in detection of certain nuclear materials required of the ASP and the potential to improve the current-generation RPM's sensitivity to nuclear materials, most likely at a lower cost.[31] DNDO officials stated that they planned to update the cost-benefit analysis; however, after spending more than $200 million on the program, in February 2010, DHS announced that it was scaling back its plans for development and use of the ASP, and subsequently announced in July 2011 that it was ending the ASP program, which means DHS continues to face limitations in radiation detection. Since DNDO continued ASP testing through 2011, GAO has ongoing work to review, among other things, the results of testing of ASP since 2009, lessons learned from the ASP program, and whether DNDO plans to conduct additional ASP testing in the future.[32]

Since 2005, DNDO was also engaged in trying to develop a more advanced nonintrusive inspection equipment system in order to detect nuclear materials that might be heavily shielded. In September 2010, we reported that DNDO was simultaneously engaged in the research and development phase while planning for the acquisition phase of its cargo advanced automated radiography system (CAARS) to detect certain

[30] GAO, *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors*, GAO-09-804T (Washington, D.C.: June 25, 2009).

[31] GAO, Homeland Security: *DHS Could Strengthen Acquisition and Development of New Technologies*, GAO-11-829T (Washington, D.C.: July 15, 2011).

[32] We are conducting this work for the ranking members of the Subcommittee on Investigations and Oversight and Subcommittee on Energy and Environment; Committee on Science, Space, and Technology; House of Representatives.

nuclear materials in vehicles and cargo containers at ports.[33] 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. We reported that this occurred because, during the first year or more of the program, DNDO and CBP had few discussions about operating requirements. DHS spent $113 million on the program since 2005 and canceled the development phase of the program in 2007.

CBP Works with Foreign Governments, the Private Sector, and International Organizations to Implement Supply Chain Security Efforts

As part of its risk-management approach, CBP operates two voluntary security programs—the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT).[34] CSI, through partnerships with CBP's foreign counterparts, is designed to target and examine high-risk container cargo as early as possible in the global supply chain. CSI places CBP officers at select foreign seaports to work with host-country customs officials to identify and scan high-risk cargo before it is shipped to the United States. CBP launched CSI in January 2002, and in fiscal year 2007 CBP reached its goal of operating CSI in 58 foreign seaports, and as of October 2011, these ports collectively accounted for over 80 percent of the cargo containers shipped to the United States. In 2005 and 2008, we made recommendations to CBP to further strengthen the CSI program by, among other things, revising its staffing model, developing performance measures, and improving processes for gathering information. CBP generally agreed and took action to implement these recommendations.[35] For example, in response to one of our recommendations, in January 2009, CBP began transferring CSI staff from overseas ports to perform targeting remotely from the National Targeting Center-Cargo in the United States. As part of this

[33] 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).

[34] For more information on CSI and C-TPAT, see GAO, *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain,* GAO-08-538 (Washington, D.C.: Aug. 15, 2008).

[35] GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed,* GAO-08-187 (Washington, D.C.: Jan. 25, 2008) and GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*. GAO-05-557 (Washington, D.C.: Apr. 26, 2005).

effort, foreign staffing levels for CSI decreased from 170 in January 2009 to 86 in April 2011 while 32 positions were added to the National Targeting Center – Cargo. As a result of the changes in its overseas staffing model, CBP has experienced a decrease in operating costs of over $35 million from fiscal year 2009 through fiscal year 2011.

While the CSI program involves partnerships between CBP and foreign governments, the C-TPAT program is a government-to-business partnership program that provides benefits to supply chain companies that comply with predetermined security measures. Under C-TPAT, CBP officials work with private companies to review their supply chain security plans and improve members' security measures. In return, C-TPAT members may receive benefits, such as reduced scrutiny or expedited processing of their shipments. CBP initiated C-TPAT in November 2001, and as of November 2010, CBP had awarded initial C-TPAT certification—or acceptance of the company's agreement to voluntarily participate in the program[36]—to over 10,000 companies.[37] C-TPAT certified members are then subject to validation whereby CBP verifies that the members' security measures meet or exceed CBP's minimum security requirements. We previously reported that C-TPAT provides CBP with a level of information sharing that would otherwise not be available from nonmember companies.[38] In 2008, we made recommendations to CBP to strengthen C-TPAT program management, in part, by developing performance measures and improving the process for validating security practices of C-TPAT members. CBP has since implemented these recommendations.[39]

CBP also partners with international trade and security groups to develop supply chain security standards that can be implemented by the

[36] Acceptance occurs after a review of the company's security profile and compliance with customs laws and regulations.

[37] Aside from maritime container shippers, C-TPAT members include many top air carriers and freight forwarders.

[38] 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).

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

international community. In 2005, the WCO developed the Framework of Standards to Secure and Facilitate Global Trade—commonly referred to as the SAFE Framework—for which the core concepts are based on components of CBP's CSI and C-TPAT programs. As of the publication of the most recent edition of the SAFE Framework in June 2011, 164 of the 177 WCO member countries have pledged to adopt the framework. As part of the SAFE framework, customs administrations may develop Authorized Economic Operator programs that offer incentives to supply chain companies that comply with predetermined minimum security standards. For example, C-TPAT is the designated Authorized Economic Operator program for the United States. According to data from the WCO, as of May 2011, 59 countries, including the 27 member states of the European Union, have implemented or have begun developing Authorized Economic Operator programs.[40]

CBP and the WCO anticipate that widespread adoption of these standards could eventually lead to a system of mutual recognition whereby the security-related practices and programs taken by the customs administration of one country are recognized and accepted by the administration of another. According to CBP, a system of mutual recognition could lead to greater efficiency in providing security by, for example, reducing redundant examinations of container cargo and avoiding the unnecessary burden of addressing different sets of requirements as a shipment moves through the supply chain in different countries. As of June 2011, CBP has signed five Mutual Recognition Arrangements and is currently working toward two more with other customs administrations, according to CBP.[41]

[40] For more information on the WCO Authorized Economic Operator Program, see World Customs Organization, *Compendium of Authorized Economic Operator Programme,.* 2011 edition.

[41] CBP has signed the five Mutual Recognition Agreements with customs administrations of New Zealand, Canada, Jordan, Japan, and South Korea and is working toward more with those of Singapore and EU. For more information, see Department of Homeland Security, Customs and Border Protection, "Mutual Recognition Information," Customs-Trade Partnership Against Terrorism website, (June 2011), accessed January 24, 2012, www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/mr/.

As The Deadline for 100 Percent Scanning Approaches, Uncertainty Persists over the Future of 100 Percent Scanning

The Scope of the Secure Freight Initiative Has Decreased after Facing Numerous Challenges

In response to the SAFE Port Act requirement to implement a pilot program to determine the feasibility of scanning 100 percent of U.S.-bound containers with both radiation detection and nonintrusive equipment, CBP, the Department of State, and the Department of Energy jointly announced the formation of the Secure Freight Initiative (SFI) pilot program in December 2006. CBP selected three ports to implement the SFI pilot program: Qasim, Pakistan; Puerto Cortes, Honduras; and Southampton, United Kingdom.

In October 2009, we reported that while CBP and the Department of Energy had made progress in integrating new technologies as part of the SFI program, progress in implementing and expanding the scanning of U.S.-bound cargo containers at participating ports was limited. Specifically, according to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement to implement the program at three ports,[42] CBP also selected the ports of Hong Kong; Busan, South Korea; and Salalah, Oman to more-fully demonstrate the capability of the integrated scanning system at larger, more complex ports with higher percentages of transshipment container cargo—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. However, these ports faced numerous challenges in implementing the 100 percent scanning requirement, as we reported in October 2009, and some ports that initially agreed to participate in the SFI program did so for a limited time, or on a limited basis.[43] For example, the SFI program began

[42] The act required CBP to identify three distinct ports through which containers pass or are transshipped to the United States with unique features and differing levels of trade volume. 6 U.S.C. § 981(a).

[43] GAO-10-12.

operating in one of the nine terminals at the port of Hong Kong in January 2008 and ended in April 2009. The SFI program was not renewed at the port of Hong Kong based on a mutual decision by the Hong Kong government and DHS, in part, because of concerns that equipment and infrastructure costs, as well as costs to port efficiency, would make full implementation of the SFI program at all of its terminals unfeasible. CBP has since reduced the scope of the SFI program, and currently the only port that continues to operate under SFI protocols is Qasim, Pakistan.

Logistical, technological, and other problems at participating ports have prevented any of the participating ports from achieving 100 percent scanning, as ultimately required by the 9/11 Act, leaving the feasibility and efficacy of 100 percent scanning largely unproven. For example, we reported in October 2009 that while CBP had been able to scan a majority of U.S.-bound cargo containers from three comparatively low-volume ports (Qasim, Puerto Cortes, and Southampton), at the higher volume ports of Hong Kong and Busan, CBP had been able to scan no more than 5 percent of U.S.-bound cargo containers, on average. Additionally, scanning operations at the initial SFI ports encountered a number of challenges—including safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images. Furthermore, since the 9/11 Act did not specify who is to conduct the container scans or who is to pay for scanning equipment or operations and maintenance, questions persist regarding who will bear the costs of scanning.

In addition to the challenges CBP faced in implementing 100 percent scanning at the select SFI pilot ports, CBP also faces a number of potential challenges in integrating the 100 percent scanning requirement with the existing container security programs that make up CBP's layered security strategy. The 100 percent scanning requirement is a departure from existing container security programs in that it requires that all containers be scanned before CBP determines their potential risk level.[44] Senior CBP officials and international trading partners say this change differs from the risk-based approach based on international supply chain security standards and accepted practices. Specifically, as we reported in October 2009 and October 2010, foreign government officials have

[44] For more information regarding the application of risk-management principles as they relate to 100 percent scanning, see GAO, *Maritime Security: Responses to Questions for the Record*, GAO-11-140R (Washington, D.C.: Oct. 22, 2010), 17-20.

expressed the view that 100 percent scanning is not consistent with risk-management principles as contained in the SAFE Framework.[45] For example, European and Asian customs officials we spoke with told us that the 100 percent scanning requirement is in contrast to the risk-based strategy, which serves as the basis for other U.S. programs, such as CSI and C-TPAT. Further, the WCO, which represents 177 customs agencies around the world, stated that the implementation of 100 percent scanning would be "tantamount to abandonment of risk management." Some foreign governments have stated they may adopt a reciprocal requirement that all U.S.-origin containers be scanned, which would present additional challenges at domestic U.S. ports.

We recommended that CBP perform analyses to determine whether 100 percent scanning is feasible, and if so, the best way to achieve it; or, alternatively, if it is not feasible, present acceptable alternatives. To date, however, CBP has not conducted such a feasibility assessment. CBP has not pursued a feasibility assessment, in part, due to the interagency effort to develop the recently issued *National Strategy for Global Supply Chain Security*. CBP officials told us in August 2011 that the agency's position was that a risk-based approach to global supply chain security was a more feasible and responsible approach than 100 percent scanning.[46] Further, CBP has not provided any details about any alternatives to 100 percent scanning that DHS or CBP may be considering.

DHS Intends to Issue a Blanket Extension Because 100 Percent Scanning Cannot be Implemented by the July 2012 Deadline

CBP's budget documents and public statements from DHS and CBP officials, along with the elimination of SFI operations at all but one port, indicate that DHS and CBP are no longer pursuing efforts to implement 100 percent scanning at foreign ports by July 2012. While CBP had previously implemented the SFI program and protocols for 100 percent scanning at six ports, it has reverted all but one of these ports to CSI operations, for which CBP focuses its efforts on scanning those cargo containers it identifies as high risk rather than requesting scans of all

[45] GAO-10-12 and GAO-11-140R.

[46] Additionally, according to CBP, the current SFI budget is focused on maintaining operations at the remaining SFI port in Qasim, Pakistan, and funds are not presently available to conduct a feasibility assessment. The current funding levels may be attributed, in part, to CBP's request to reduce funding for the SFI program. In CBP's fiscal year 2011 budget justification, CBP requested a reduction $16.6 million due to plans to revert three of the SFI ports to CSI operations.

containers regardless of risk. According to CBP's fiscal year 2011 budget justification, the SFI program is a "helpful but not essential part" of CBP's layered security strategy. In addition, the budget justification noted that DHS will continue to use and, when appropriate, strengthen other means to achieve the same goals of SFI, such as the 24-hour rule, the 10+2 rule, and C-TPAT. Further, there is no mention of the 100 percent scanning mandate or efforts to meet the mandate in the recently released *National Strategy for Global Supply Chain Security*. Rather, the strategy notes that the federal government intends to focus its efforts on "those enhancements that result in the most significant improvement or reduction in risk."

As the July 2012 deadline in the mandate approaches, uncertainty remains regarding DHS's long term course of action to satisfy the 100 percent scanning mandate. As we previously reported, in the short term, DHS acknowledged it will not be able to meet this deadline for full-scale implementation of the 9/11 Act's scanning requirement and will need to grant extensions to those foreign ports unable to meet the scanning deadline in order to maintain the flow of trade and comply with the 9/11 Act. The 9/11 Act allows DHS to grant an extension to a port or ports by certifying that least two of six conditions exist,[47] and as we previously reported, DHS believes the last two conditions—(1) use of the equipment to scan all U.S.-bound containers would significantly impact trade capacity and the flow of cargo and (2) scanning equipment does not adequately provide automatic notification of an anomaly in a container—could apply to all foreign ports that ship containers to the United States. Therefore, DHS expects to grant a blanket extension to all foreign ports pursuant to the statue, thus extending the target date for compliance with this requirement by 2 years, to July 2014. To do so, the 9/11 Act requires DHS to report to Congress 60 days before any extension takes effect on the container traffic affected by the extension, the evidence supporting

[47] The 9/11 Act scanning requirement authorizes DHS to grant extensions for a port or ports if at least two of the following six conditions exist: (1) equipment to scan all U.S.-bound containers is not available for purchase and installation; (2) equipment to scan all U.S.-bound containers does not have a sufficiently low false alarm rate; (3) equipment to scan all U.S.-bound containers cannot be purchased, deployed, or operated at a port or ports (including where this is due to the physical characteristics of the port); (4) equipment to scan all U.S.-bound containers cannot be integrated with existing systems; (5) use of the equipment to scan all U.S.-bound containers would significantly impact trade capacity and the flow of cargo; or (6) the scanning equipment does not adequately provide automatic notification of an anomaly in a container. 6 U.S.C. § 982(b)(4).

the extension, and the measures DHS is taking to ensure that scanning can be implemented as early as possible at the ports covered by the extension.[48] As a result, DHS will need to notify Congress by May 2, 2012, of any extensions it plans to grant.[49]

Given that the feasibility of 100 percent scanning remains unproven and DHS and CBP have not yet identified alternatives that could achieve the same goals as 100 percent scanning, uncertainty persists regarding the scope of DHS's and CBP's container security programs and how these programs will collectively affect the movement of goods between global trading partners.

Chairman Miller, Ranking Member Cuellar, and Members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the Subcommittee may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen L. Caldwell at 202-512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the contacts named above, Christopher Conrad, Assistant Director, managed this review. Gene Aloise, Lisa Canini, Frances Cook, Alana Finley, Rich Hung, Katie Mauldin, Jessica Orr, Janay Sam, David Schmitt, Kevin Tarmann, and Ned Woodward made key contributions to this statement.

[48] 6 U.S.C. § 982(b)(6).

[49] Additionally, 1 year after an extension takes effect, DHS would be required to submit a report on Congress on whether it expects to seek to renew the extension. 6 U.S.C. § 982(b)(7).

Related GAO Products

Homeland Security: DHS Could Strengthen Acquisitions and Development of New Technologies. GAO-11-829T. Washington, D.C.: July 15, 2011.

Maritime Security: Responses to Questions for the Record. GAO-11-140R. Washington, D.C.: October 22, 2010.

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-10-887. Washington, D.C.: September 29, 2010.

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

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.: September 15, 2010.

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

Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors. GAO-09-804T. Washington, D.C.: June 25, 2009.

Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology. GAO-09-655. Washington, D.C.: May 21, 2009.

Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain. GAO-08-538. Washington, D.C.: August 15, 2008.

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

Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed. GAO-08-187. Washington, D.C.: January 25, 2008.

Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System. GAO-06-591T. Washington, D.C.: March 30, 2006.

Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts. GAO-05-557. Washington, D.C.: April 26, 2005.