United States Government Accountability Office

Testimony

Before the Subcommittees on Coast Guard and Maritime Transportation and Border and Maritime Security, Committees on Transportation and Infrastructure and Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, July 7, 2016

MARITIME SECURITY

Progress and Challenges in Implementing Maritime Cargo Security Programs

Statement of Jennifer A. Grover, Director
Homeland Security and Justice

July 7, 2016

MARITIME SECURITY

Progress and Challenges in Implementing Maritime Cargo Security Programs

GAO Highlights

Highlights of GAO-16-790T, a testimony before the Subcommittees on Coast Guard and Maritime Transportation and Border and Maritime Security, Committees on Transportation and Infrastructure and Homeland Security, House of Representatives

Why GAO Did This Study

The U.S. economy is dependent on the expeditious flow of millions of tons of cargo each day through the global supply chain—the flow of goods from manufacturers to retailers. Criminal or terrorist attacks using cargo shipments can cause disruptions to the supply chain and can limit global economic growth and productivity. Within DHS, CBP has responsibility for administering maritime cargo security measures and reducing the vulnerabilities associated with the supply chain. CBP has developed a layered security strategy that focuses its limited resources on targeting and examining high-risk cargo shipments that could pose a risk while allowing other cargo shipments to proceed without unduly disrupting commerce arriving in the United States.

This statement discusses the progress and challenges associated with CBP's implementation of initiatives and programs responsible for enhancing the security of the global supply chain. The statement is based on reports and testimonies GAO issued from April 2008 through January 2015 related to maritime cargo security—with selected updates on how DHS has responded to GAO's prior recommendations.

What GAO Recommends

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

View GAO-16-790T. For more information, contact Jennifer A. Grover at (202) 512-7141 or groverj@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have made substantial progress in implementing initiatives and programs that, collectively, have enhanced cargo security, but some challenges remain. Examples of progress and challenges are discussed below.

Risk Assessments of Cargo Shipments. In January 2015, GAO found that CBP did not have accurate data on the number and disposition of each high-risk shipment scheduled to arrive in the United States. Specifically, CBP's data overstated the number of high-risk shipments, including those that appeared not to be examined or waived in accordance with CBP policy. CBP officers inconsistently applied criteria to make some waiver decisions and incorrectly documented waiver reasons. GAO recommended that CBP define waiver categories and disseminate policy on issuing waivers. In response, CBP issued a new policy that includes criteria for waiving examinations of high-risk shipments and developed a new process for recording waivers and issued a memorandum.

Partnerships with Foreign Governments. In September 2013, GAO reported that CBP had not regularly assessed foreign ports for risks to cargo since 2005. GAO recommended that DHS periodically assess the security risks from ports that ship cargo to the United States and use the results to inform whether changes need to be made to Container Security Initiative (CSI) ports. DHS concurred with the recommendation and CBP has since developed a port risk matrix and priority map to be used to help assess whether changes need to be made to CSI ports. These tools are to be updated yearly and can be updated more frequently based on significant changes, emerging threats, and intelligence. These tools should assist CBP in ensuring it is allocating its resources to provide the greatest coverage of U.S.-bound high-risk cargo.

In October 2009, GAO reported challenges to scanning 100 percent of U.S.-bound cargo at foreign ports. DHS officials acknowledged that most, if not all foreign ports, would not be able to meet the July 2012 target date for scanning all U.S.-bound cargo, and DHS would need to issue extensions to allow the continued flow of commerce and remain in compliance with statutory requirements. Although the Secretary of Homeland Security has issued three 2-year extensions for implementing the 100 percent scanning mandate, which have extended the deadline to July 2018, DHS has not yet identified a viable solution to meet the requirement.

Partnerships with the Trade Industry. Through the Customs-Trade Partnership Against Terrorism (C-TPAT) program, CBP officials work with member companies to validate the security of their supply chains in exchange for benefits, such as reduced scrutiny of their shipments. In April 2008, GAO found, among other things, that CBP lacked a systematic process to ensure that members take appropriate actions in response to security validations. GAO recommended that CBP document key data elements needed to track compliance. CBP has since implemented a process to ensure that C-TPAT validation report recommendations are implemented. GAO is currently reviewing the C-TPAT program, to include an assessment of CBP's ability to meet its security validation responsibilities.

Chairman Hunter, Chairwoman McSally, Ranking Members Garamendi and Vela, and Members of the Subcommittees:

Thank you for the opportunity to discuss our work on U.S. Customs and Border Protection's (CBP) initiatives and programs to enhance maritime cargo security. The U.S. economy is dependent on the expeditious flow of millions of tons of cargo each day through the global supply chain—the flow of goods from manufacturers to retailers. Cargo containers are an important segment of the global supply chain and play a vital role in the movement of cargo between global trading partners. The majority of U.S. imports arrive by ocean vessel, and much of that is shipped in the millions of cargo containers that enter the United States every year. Cargo containers can be filled overseas at many different locations and they are transported through complex logistics networks before reaching U.S. ports. Criminal or terrorist attacks using cargo shipments can cause disruptions to the supply chain and can limit global economic growth and productivity.[1] Within the Department of Homeland Security (DHS), CBP is responsible for administering cargo security and reducing the vulnerabilities associated with the supply chain. According to DHS, balancing security concerns with the need to facilitate the free flow of commerce, part of CBP's mission, remains an ongoing challenge.[2]

CBP has developed a layered security strategy to focus its limited resources on targeting and examining high-risk cargo shipments that could pose a risk while allowing other cargo shipments to proceed without unduly disrupting commerce arriving in the United States. CBP's layered security strategy is based on initiatives and programs that include, among other things, analyzing information to identify shipments that may be at high risk of transporting weapons of mass destruction (WMD) or other contraband, working with foreign governments to examine U.S.-bound shipments at foreign ports participating in the Container Security Initiative (CSI) and Secure Freight Initiative (SFI), and providing benefits to companies that comply with CBP's minimum security criteria through the

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

[2]In addition to its priority mission of keeping terrorists and their weapons out of the United States, CBP is also responsible for securing the border, facilitating international trade and travel, collecting duties, and enforcing numerous U.S. laws and regulations pertaining to immigration and illicit drugs, among other things.

Customs-Trade Partnership Against Terrorism (C-TPAT) program. The Security and Accountability for Every Port Act (SAFE Port Act) of 2006, enacted in October 2006, established a statutory framework for key programs within CBP's layered security strategy that previously had not specifically been required by law.[3] A brief description of the key initiatives and programs that constitute CBP's layered security strategy is provided in appendix I.

My statement today discusses the progress and challenges associated with CBP's implementation of maritime cargo security initiatives and programs responsible for enhancing the security of the global supply chain. This statement is based on reports and testimonies we issued from April 2008 through January 2015 related to maritime cargo security—with selected updates on how DHS and CBP have responded to our prior recommendations. The products cited in this statement provide detailed information on our scope and methodology. The work upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Every time responsibility for cargo changes hands along the global supply chain there is the potential for a security breach. As a result, vulnerabilities exist that terrorists could take advantage of by, for example, placing a WMD into a container bound for the United States. While there have been no known incidents of containers being used to transport WMD, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. To address the potential security risks posed by the millions of containers that arrive in the United States each year, CBP has implemented a layered security strategy of related initiatives and programs that focus CBP's limited resources on potentially high-risk cargo bound for the United States while allowing other cargo to proceed without unduly

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

disrupting commerce. Key elements of CBP's maritime cargo security initiatives and programs are described below.

Automated Targeting System. Information on shipments destined for the United States is automatically fed into CBP's Automated Targeting System (ATS)—an enforcement and decision support system that compares cargo information against intelligence and other law enforcement data. ATS consolidates data from various sources to create a single, comprehensive record for each U.S.-bound shipment. ATS uses a set of rules that assess different factors in the information to determine the risk level of a shipment. One set of rules within ATS, referred to collectively as the maritime national security weight set, is programmed to check for information or patterns that could be indicative of suspicious or terrorist activity. ATS uses this weight set to assess and generate risk scores for every cargo shipment as the shipment moves throughout the global supply chain and new information is provided or existing information is revised. CBP classifies the risk scores from the maritime national security weight set as low, medium, or high risk. ATS automatically places high-risk shipments on hold, and CBP officials use information in ATS to identify (target) which high-risk shipments should be examined or waived.

To assist in its targeting efforts, CBP uses key information about shipments destined for the United States obtained through the 24-hour rule and the 10+2 rule. Through the 24-hour rule, CBP generally requires vessel carriers to electronically transmit cargo manifests to CBP 24 hours before cargo is loaded onto U.S.-bound vessels at foreign ports.[4] Through the Importer Security Filing and Additional Carrier Requirements (known as the 10+2 rule), CBP requires importers and vessel carriers to provide data elements for improved identification of cargo shipments that may pose a risk for terrorism.[5] Importers are responsible for supplying CBP with 10 shipping data elements—such as country of origin—24 hours prior to loading, while vessel carriers are required to provide 2 data

[4]19 C.F.R. § 4.7(b). Cargo manifests are prepared by the ocean carrier and are composed of bills of lading for each shipment loaded onto a vessel to describe the contents of the shipments. Bills of lading are documents issued by a carrier describing the goods, the details of the intended voyage, and the conditions of transportation.

[5]Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (codified at 19 C.F.R. pt. 149).

elements—container status messages and stow plans—that are not required by the 24-hour rule.[6]

Container Security Initiative. CSI is a bilateral government partnership program operated by CBP that aims to identify and examine U.S.-bound cargo container shipments that are at risk of containing WMD or other terrorist contraband. As part of the program, CBP officers are stationed at select foreign seaports and review information about U.S.-bound containerized cargo shipments. CBP uses ATS to target U.S.-bound container shipments and request examinations of high-risk container shipments before they are loaded onto vessels. CSI is operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP estimates that, through the CSI program, it prescreens over 80 percent of all maritime containerized cargo imported into the United States.

Secure Freight Initiative. In response to a requirement in the SAFE Port Act to scan 100 percent of U.S.-bound cargo containers, CBP established SFI.[7] CBP uses radiation detection and non-intrusive inspection equipment to scan cargo containers before they are loaded onto vessels at select foreign seaports Radiation detection equipment, such as radiation portal monitors (RPM) and radiation isotope identification devices (RIID) detect the presence of radioactive material that may be in a container. RIIDs and certain types of RPMs can identify the specific radioactive isotope being emitted and whether the radiation is a threat or is naturally occurring, such as that found in certain ceramic tiles. The second type of equipment, referred to as non-intrusive inspection equipment, uses X-rays or gamma rays to scan a container and produce images of a container's contents without having to open it.

Customs-Trade Partnership Against Terrorism. C-TPAT is a voluntary, public-private sector partnership with private stakeholders in the

[6]Container status messages report terminal container movements, such as loading and discharging the vessel, and report the change in the status of containers, such as if they are empty or full. Container status messages also report conveyance movements, such as vessel arrivals and departures. A vessel stow plan includes information such as the vessel operator, voyage number, the stow position of each container, hazardous material code (if applicable), and the port of discharge.

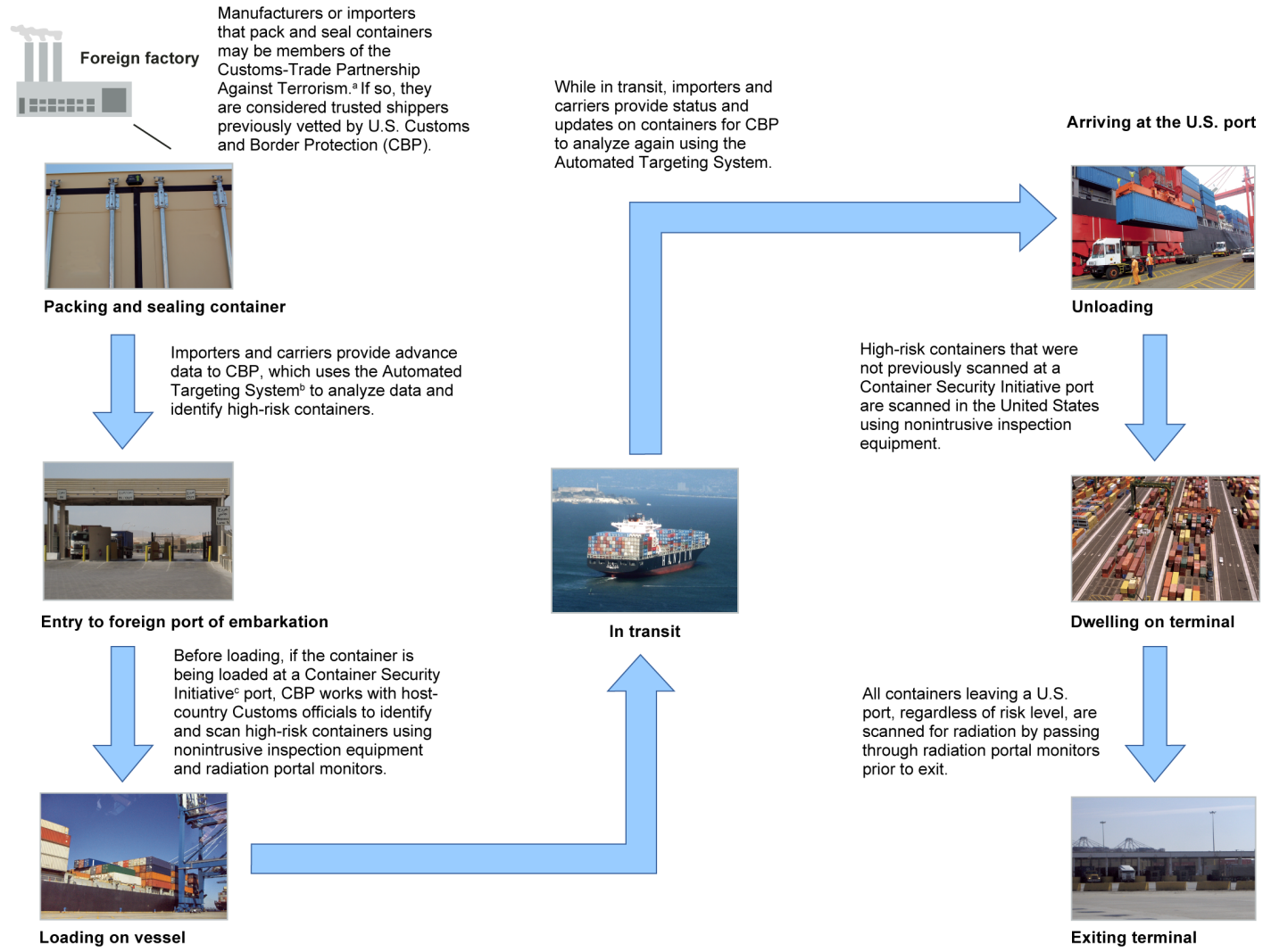
[7]See 6 U.S.C. §§ 981-82.

international trade community that aims to secure the flow of maritime cargo bound for the United States.[8] Through C-TPAT, CBP officials work with member private companies to review the security of their supply chains to ensure their security practices meet CBP's minimum security criteria. In return, C-TPAT members receive various benefits, such as reduced scrutiny of their shipments.

Figure 1 provides an overview of the global supply chain and the steps in the supply chain where CBP's key initiatives and programs come into play.

[8]See 6 U.S.C. § 961.

Figure 1: The Global Supply Chain and CBP's Key Cargo Security Initiatives and Programs



Source: GAO (analysis); GAO and Department of Homeland Security Science and Technology Directorate (photos); Art Explosion (clipart). | GAO-16-790T

[a]The Customs-Trade Partnership Against Terrorism is a voluntary program designed to improve the security of the 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 it is shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that the officials' foreign counterparts examine the contents of the containers.

CBP Has Made Substantial Progress in Enhancing Cargo Security, but Some Challenges Remain

Our prior work has shown that CBP has made substantial progress in implementing various initiatives and programs that, collectively, have enhanced cargo security, but some challenges remain. Examples of progress and challenges in the areas of (1) using information for improving targeting and risk assessment of cargo shipments, (2) partnerships with foreign governments, and (3) partnerships with the trade industry are discussed below.

CBP's Efforts to Improve Targeting and Risk Assessments of Cargo Shipments

In January 2015, we found, among other things, that CBP did not have accurate data on the number and disposition of each high-risk maritime cargo shipment scheduled to arrive in the United States.[9] On the basis of our analyses of CBP data for fiscal years 2009 through 2013, we found that, on average each year, approximately 11.6 million maritime cargo container shipments arrived in the United States, and less than 1 percent of those shipments were determined by ATS to be high-risk. We found that CBP examined the vast majority of high-risk shipments, but CBP's data on the disposition of high-risk shipments were not accurate because of various factors, such as the inclusion of shipments that were never sent to the United States. Further, our analyses found that CBP's data overstated the number of high-risk shipments, including those that appeared not to be resolved (examined or waived) in accordance with CBP policy. We also found that when determining the disposition of high-risk shipments, CBP officers were inconsistently applying criteria to make some waiver decisions and were also incorrectly documenting the reasons for waivers.[10] As a result, we concluded that CBP could not accurately determine the extent to which waivers were used consistently and judiciously across CBP targeting units, as required by policy. We recommended, among other things, that CBP define waiver categories

[9]GAO, *Supply Chain Security: CBP Needs to Enhance Its Guidance and Oversight of High-Risk Maritime Cargo Shipments*, GAO-15-294 (Washington, D.C.: Jan. 27, 2015).

[10]CBP officers can waive an examination if they determine through research that (1) the shipment falls within a predetermined category of stated exceptions (standard exception), or (2) they can articulate why the shipment should not be considered high-risk (articulable reason). For example, a shipment could be identified as high-risk because it is associated with a shipper on a terrorist watch list, but through further research, CBP officials determine the shipper is not a true match to the terrorist watch list and, therefore, the shipment should not be considered high-risk.

and disseminate policy on issuing waivers for high-risk shipments. DHS concurred with our recommendations and, in December 2015, CBP issued a new policy, *National Security Cargo Targeting Procedures*, that includes criteria for waiving mandatory examinations of high-risk shipments (referred to as exceptions). The new policy also specifically identifies certain types of shipments that do not qualify for exceptions to examination requirements. In addition, CBP developed a new process for recording waivers and issued a memorandum to targeting units on how to apply the new procedures. CBP's actions help ensure that all of its targeting units are correctly and consistently applying and documenting waivers.

In October 2012, we found that more regular assessments of ATS were needed to enhance CBP's targeting of maritime cargo and better position CBP to provide reasonable assurance of the effectiveness of ATS.[11] We, therefore, recommended that CBP (1) ensure that future updates to the rules that identify risks are based on results of assessments that demonstrate the effectiveness of such updates; and (2) establish targets for CBP's performance measures and use those measures to assess the effectiveness of ATS on a regular basis to better determine when updates to the rules that identify risks are needed. DHS concurred with the recommendations and, in May 2015, CBP revised its *National Security Weight Set, Maritime Standard Operating Procedures* (SOP) to address the new requirements for the maintenance, review, and update of the national security weight set in ATS. The SOP requires program managers to compare proposed versions of the national security weight set against the existing version as part of the process for determining whether to implement a proposed new version of the weight set. Doing so will help provide reasonable assurance that changes to the weight set will improve the effectiveness of CBP's targeting of maritime cargo container shipments. The SOP also establishes a performance measure and an associated target that will assist CBP in determining whether the weight set is effectively targeting maritime cargo container shipments. The SOP requires CBP to review the national security weight set for revisions if the weight set does not meet the performance target in two consecutive quarters. By assessing the weight set regularly against a performance

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

target, CBP will be better positioned to determine when updates to the weight set are needed to ensure continued effectiveness in targeting of high-risk maritime cargo container shipments.

In September 2010, we reviewed CBP's efforts to collect additional data through the 10+2 rule and utilize these data to identify high-risk shipments.[12] We found that the 10+2 rule data elements were available for identifying high-risk cargo, but CBP had not yet finalized its national security targeting criteria to include these additional data elements to support high-risk targeting. We recommended that CBP establish milestones and time frames for updating the targeting criteria. In December 2010, CBP provided us with a project plan for integrating the data into its criteria, and in January 2011, CBP implemented the updates to address risk factors present in the 10+2 data. We are currently reviewing CBP's implementation and enforcement of the 10+2 program and anticipate issuing our report in spring 2017.

CBP's Partnerships with Foreign Governments

In September 2013, we reported on CBP's progress in implementing CSI.[13] Specifically, we found that CBP had not regularly assessed foreign ports for risks to cargo under the CSI program since 2005. While CBP took steps to rank ports for risks in 2009, we found that CBP did not use results from this assessment to make modifications to the locations where CSI staff are posted because of budget cuts. By applying CBP's risk model to fiscal year 2012 cargo shipment data, we found that CSI did not have a presence at about half of the foreign ports CBP considered high-risk, and about one-fifth of the existing CSI ports were at lower-risk locations. We recommended that DHS periodically assess the supply chain security risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to inform any future expansion of CSI to additional locations and determine whether changes need to be made to existing CSI ports and make adjustments as appropriate and feasible. DHS concurred with our recommendation and,

[12]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).

[13]GAO, *Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports,* GAO-13-764 (Washington, D.C.: Sept. 16, 2013).

in response, CBP developed a CSI Port Risk Matrix and Port Priority Map. CBP officials stated that the matrix and map will be used, along with several other tools available to CSI, to assess whether changes need to be made to CSI ports worldwide. According to CBP, these tools are to be updated yearly and, if necessary, can be updated more frequently based on significant changes, emerging threats, and intelligence. As a result of developing and employing these new risk-assessment tools, CBP should be better positioned to ensure that it is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing WMD or other terrorist contraband into the United States through the supply chain.

In October 2009, we reported that 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.[14] Both CBP and GAO had previously identified many of these challenges, and CBP officials were concerned that they and the participating ports could not overcome them. Senior DHS and CBP officials acknowledged that most, if not all foreign ports, would not be able to meet the July 2012 target date for scanning all U.S.-bound cargo, and DHS would need to issue extensions to such ports to allow the continued flow of commerce in order to remain in compliance with relevant statutory requirements.[15] We recommended that DHS, in consultation with the Secretaries of Energy and State, develop, among other things, more comprehensive cost estimates, conduct cost-benefit and feasibility analyses, and provide the results to Congress. In response to our recommendations, CBP stated it had no plans to develop comprehensive cost estimates or feasibility analyses since SFI is operating at one port and it had no funds to conduct

[14]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).

[15]Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007, which established the July 2012 deadline for 100 percent scanning of containers loaded in a port or ports, this deadline may be extended in two-year increments if DHS certifies to Congress that at least two out of a list of specific conditions exist. Among others, these conditions include the following: adequate scanning equipment is not available or cannot be integrated with existing systems, a port does not have the physical characteristics to install the equipment, or use of the equipment will significantly affect trade capacity and the flow of cargo. See 6 U.S.C. § 982(b)(4).

such analyses. In July 2013, we closed these recommendations as not implemented.

In May of 2012, 2014, and 2016, the Secretary of Homeland Security authorized a 2-year extension of the deadline for implementing the 100 percent scanning requirement for U.S. bound cargo before it is loaded onto vessels at foreign seaports. In May 2014, the Secretary of Homeland Security renewed the extension (until July 2016) and stated that "DHS's ability to fully comply with this unfunded mandate of 100 percent scanning, even in [the] long term, is highly improbable, hugely expensive, and in our judgment, not the best use of taxpayer resources to meet this country's port security and homeland security needs." The Secretary also stated that he instructed DHS, including CBP, to do a better job of meeting the underlying objectives of the mandate. In the most recent letter, dated May 2016, authorizing the extension until July 2018, the Secretary stated he has committed the Department to work towards meeting the mandated 100 percent scanning requirement. The Secretary also outlined steps DHS is taking to engage stakeholders to identify solutions by leveraging the private sector. DHS plans to assess the feedback it receives during the summer of 2016 and will subsequently seek to test viable solutions in operational environments.

CBP's Partnerships with the Trade Industry

In April 2008, we reported, among other things, that CBP took steps to improve the process for validating C-TPAT applicants' security practices and implemented numerous actions to address C-TPAT management and staffing challenges.[16] However, we found challenges with the technology CBP used to help ensure that validation information is consistently collected, documented, and uniformly applied to decisions regarding the awarding of benefits to C-TPAT members, and that CBP lacked a systematic process to ensure that members take appropriate actions in response to security validation findings. We also found that C-TPAT's performance measures were insufficient to assess the impact of C-TPAT on increasing supply chain security. We made recommendations to CBP to strengthen C-TPAT program management and oversight. Specifically, we recommended, among other things, that CBP document

[16]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).

key data elements needed to track compliance with the SAFE Port Act and other CBP internal requirements and to identify and pursue opportunities in information collected during C-TPAT member processing activities that may provide direction for developing performance measures of enhanced supply chain security. CBP has since implemented these recommendations by, for example, creating an automated platform to track and capture the content and communication between CBP and C-TPAT members to ensure that C-TPAT validation report recommendations are implemented and identifying analytical tools and data for trend analysis to better assess C-TPAT's impact on the supply chain. We are currently reviewing the C-TPAT program, specifically how CBP assesses member benefits and conducts security validation responsibilities. We anticipate issuing our report in late fall 2016.

Thank you Chairman Hunter, Chairwoman McSally, Ranking Members Garamendi and Vela, and Members of the Subcommittees. This completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Christopher Conrad (Assistant Director), Carla Brown, Lisa Canini, Michele Fejfar, Eric Hauswirth, Heidi Nielson, Ashley Rawson, and Natarajan Subramanian. Key contributors for the previous work that this testimony is based on are listed in those products.

Appendix I: Description of CBP's Layered Security Strategy for Maritime Cargo Shipments

This appendix describes the key initiatives and programs related to U.S. Customs and Border Protection's (CBP) strategy for ensuring the security of maritime cargo. CBP has developed this strategy to mitigate the risk of weapons of mass destruction, terrorist-related material, or other contraband from being smuggled into the United States. CBP's strategy is based on related initiatives and programs that attempt to focus resources on high-risk shipments while allowing other cargo shipments to proceed without unduly disrupting the flow of commerce into the United States. The strategy includes obtaining cargo information on shipments in advance of their arrival at U.S. ports to identify high-risk shipments, using technology to inspect cargo, and partnering with foreign governments and members of the trade industry. Table 1 provides a brief description of some of the key initiatives and programs that compose this security strategy.

Table 1: Description of U.S. Customs and Border Protection's (CBP) Key Cargo Security Initiatives and Programs

Initiative/program and year introduced	Description
Obtaining advanced information to identify high-risk cargo	
Automated Targeting System (ATS), 1999	ATS is an enforcement and decision support system that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. ATS assigns a risk score to arriving cargo shipments based on shipping information to help CBP identify and prevent potential terrorists and terrorist weapons from entering the United States.
24-hour rule, 2002	CBP generally requires vessel carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before U.S.-bound cargo is loaded onto a vessel at a foreign port. The information is used by ATS in its calculation of risk scores. The cargo manifest information is submitted by vessel carriers for all arriving cargo shipments.
Importer Security Filing and Additional Carrier Requirements (also known as the 10+2 rule), 2009	CBP requires importers and vessel carriers to provide data elements for improved identification of containerized shipments that may pose a risk for terrorism. The importer is responsible for supplying CBP with 10 shipping data elements, such as country of origin, 24 hours prior to loading, while the vessel carrier is required to provide 2 data elements, container status messages and stow plans, not required by the 24-hour rule.[a]
Domestic scanning technology deployments	
Non-intrusive inspection (NII) equipment, 2001	CBP uses NII equipment to actively scan both randomly selected containers and those identified by ATS as high risk. NII uses X-rays or gamma rays to scan a container and create images of the container's contents without opening it. According to CBP, as of August 2014, it had deployed 272 large-scale NII systems to U.S. seaports to scan containers.
Radiation portal monitors (RPM), 2002	CBP's program to scan 100 percent of containers arriving in the United States with radiation detection equipment prior to leaving a domestic port. As of August 2014, the Department of Homeland Security (DHS) had deployed 388 radiation portal monitors at U.S. seaports, through which over 99 percent of all containerized cargo arriving by sea is scanned.
Partnerships with foreign governments and the trade industry	

Container Security Initiative, 2002	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. CBP officials identify the containers that may pose a risk for terrorism and request that their foreign counterparts examine the contents of the containers. As of July 2014, there were 58 Container Security Initiative ports located in 32 countries.
Secure Freight Initiative (SFI), 2007	CBP initiative to scan 100 percent of U.S.-bound container cargo for nuclear and radiological materials at selected foreign ports using integrated examination systems that couple NII and radiation detection equipment before being placed on U.S.-bound vessels.[b] SFI was originally operational at six ports, but has since been reduced in scope and is only operational at one port.
Customs-Trade Partnership Against Terrorism, 2001	CBP develops voluntary partnerships with members of the international trade community composed of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies that implement specific security measures and best practices receive facilitated processing, such as a reduced likelihood of security-based examinations of their cargo.

Source: GAO summary of information provided by the Department of Homeland Security. I GAO-16-790T.

[a]Container status messages report terminal container movements, such as loading and discharging the vessel, and report the change in the status of a container, such as if it is empty or full. The stow plan provides information on the position of each cargo container on a vessel.

[b]See 6 U.S.C. § 982 (stating the July 2012 deadline for 100 percent scanning of containers loaded in a port or ports, and allowing this deadline to be extended in two-year increments if DHS certifies to Congress that at least two out of a list of specific conditions exist).