



September 2013

SUPPLY CHAIN SECURITY

DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports

GAO Highlights

Highlights of [GAO-13-764](#), a report to congressional requesters

Why GAO Did This Study

Foreign ports and the cargo carried by vessels from these ports are critical to the U.S. economy, but can be exploited by terrorists. Within DHS, CBP and the Coast Guard are responsible for maritime security. Through CSI, CBP identifies and examines U.S.-bound cargo that may conceal WMD, and through C-TPAT, CBP partners with international trade community members to secure the flow of U.S.-bound goods. Under the IPS program, Coast Guard officials visit foreign ports to assess compliance with security standards. GAO was asked to review DHS's maritime security programs. This report addresses (1) the extent to which DHS has assessed the foreign ports that pose the greatest risk to the global supply chain and focused its maritime container security programs to address those risks, and (2) actions DHS has taken to help ensure the efficiency and effectiveness of its maritime security programs. GAO analyzed DHS risk models and maritime security program strategies, met with program officials, and visited six foreign countries selected on the basis of participation in CSI, varied cargo shipment risk levels, and other factors.

What GAO Recommends

GAO recommends that CBP periodically assess the supply chain security risks from foreign ports that ship cargo to the United States and use the results to inform any future expansion of CSI and determine whether changes need to be made to existing CSI ports. DHS concurred with GAO's recommendation.

View [GAO-13-764](#). For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov

September 2013

SUPPLY CHAIN SECURITY

DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports

What GAO Found

Department of Homeland Security (DHS) components have developed models to assess the risks of foreign ports and cargo, but not all components have applied risk management principles to assess whether maritime security programs cover the riskiest ports. The U.S. Coast Guard uses its risk model to inform operational decisions for its International Port Security (IPS) program and annually updates its assessment. In contrast, U.S. Customs and Border Protection (CBP) has not regularly assessed ports for risks to cargo under its Container Security Initiative (CSI) program. CBP's selection of the initial 23 CSI ports was primarily based on the volume of U.S.-bound containers, but beginning in 2003, CBP considered more threat information when it expanded the number of CSI ports. CBP has not assessed the risk posed by foreign ports that ship cargo to the United States for its CSI program since 2005. In 2009, CBP developed a model that ranked 356 potential expansion ports for a related program on the basis of risk, but it was never implemented because of budget cuts. By applying CBP's risk model to fiscal year 2012 cargo shipment data, GAO found that CSI did not have a presence at about half of the ports CBP considered high risk, and about one fifth of the existing CSI ports were at lower risk locations. Since the CSI program depends on cooperation from sovereign host countries, there are challenges to implementing CSI in new foreign locations, and CBP's negotiations with other countries have not always succeeded. For example, CBP officials said it is difficult to close CSI ports and open new ports because removing CSI from a country might negatively affect U.S. relations with the host government. However, periodically assessing the risk level of cargo shipped from foreign ports and using the results to inform any future expansion of CSI to additional locations, as well as determine whether changes need to be made to existing CSI ports, would help ensure that CBP is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing weapons of mass destruction (WMD) or other terrorist contraband into the United States through the maritime supply chain.

DHS has taken steps to improve the efficiency and effectiveness of its maritime security programs, but faces host country political and legal constraints. The Coast Guard has implemented a risk-informed model that prioritizes the countries to visit and assist. Also, the Coast Guard and CBP have made arrangements with foreign government entities to mutually recognize inspections of each other's ports and maritime supply chains through the IPS and Customs-Trade Partnership Against Terrorism (C-TPAT) programs. CBP has also utilized technological improvements to target some U.S.-bound cargo shipments remotely from the United States to reduce CSI staff in foreign countries. However, CBP faces political and legal constraints in host countries. For example, according to CBP and government officials in one country, a national law precludes the transmission of electronic scanned images other than to host government Customs officials. As a result, CSI officials must be present at each CSI port in that country to view the scanned images. Further, in some ports, CBP has made efforts to expand the scope of its CSI targeting to include contraband other than WMD, but that is subject to approval by the host governments.

Contents

Letter		1
	Background	7
	DHS Has Developed Models to Assess Foreign Port Risks, but CBP Has Not Assessed Whether Its CSI Locations Remain Valid	16
	DHS Has Taken Steps to Improve the Efficiency and Effectiveness of Its Maritime Container Security Programs, but Faces Constraints	24
	Conclusions	37
	Recommendations for Executive Action	37
	Agency Comments and Our Evaluation	38
Appendix I	Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection	39
Appendix II	Comments from the Department of Homeland Security	42
Appendix III	GAO Contact and Staff Acknowledgments	44
Related GAO Products		45
Tables		
	Table 1: Coast Guard International Port Security Program Visits, by Country Risk Level, for Fiscal Year 2012	26
	Table 2: Foreign Ports That CBP Coordinates with Regarding Maritime Container Shipment Examinations, as of July 2013 (Listed by Date Port Began CSI Operations)	39
Figures		
	Figure 1: Illustrative Example of Key Points in the Global Supply Chain	8
	Figure 2: Department of Homeland Security's (DHS) Key Maritime Security Programs	9

Figure 3: Panama Customs Examining a Container Using Imaging Equipment, Port of Balboa, Panama	11
Figure 4: Partial View of the Port of Singapore	19
Figure 5: Map Showing the Variety of Targeting Approaches Customs and Border Protection Uses in Container Security Initiative Countries as of July 2013	33

Abbreviations

AEO	authorized economic operator
ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOE	Department of Energy
IPS	International Port Security program
ISPS Code	International Ship and Port Facility Security Code
MOU	memorandum of understanding
MRA	mutual recognition arrangement
MTSA	Maritime Transportation Security Act
NTC-C	National Targeting Center-Cargo
SAFE Port Act	Security and Accountability for Every Port Act
WMD	weapons of mass destruction

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 16, 2013

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
United States Senate

Foreign ports and the cargo carried by vessels from these ports are critical to the U.S. economy but can also be exploited by terrorists. According to the U.S. Department of Transportation, the majority of U.S. imports arrive by ocean vessel, and much of that is transported in cargo containers.¹ Cargo containers are an important segment of the global supply chain—the flow of goods from manufacturers to retailers—and can present significant security concerns. For example, a 2012 risk assessment by the Department of Homeland Security (DHS) found that attacks could cause major disruptions to the maritime supply chain. DHS officials believe that the likelihood of terrorists smuggling weapons of mass destruction (WMD) into the United States in cargo containers is relatively low; however, the consequences of such an event could be catastrophic. Although there have been no known incidents of cargo containers being used to transport WMD, ensuring the security of cargo containers remains an important role for the federal government given that criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. To balance the government's need to help secure the global supply chain while also promoting the efficient and secure movement of goods, the White House issued the National Strategy for Global Supply Chain Security in January 2012, which emphasizes a risk-informed approach for DHS's cargo security programs across all modes of transportation.² This strategy

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

²The White House, *National Strategy for Global Supply Chain Security* (Washington, D.C.: January 2012).

builds on a number of strategic efforts to strengthen the global supply chain.³ While DHS' cargo security programs cover all modes of transportation, the focus of this report is on DHS's maritime security programs.

In the federal government, U.S. Customs and Border Protection (CBP) and the Coast Guard, both within DHS, are two key agencies responsible for maritime security issues. In particular, CBP is responsible for, among other things, assessing the overall security of the supply chain and reducing the vulnerabilities associated with U.S.-bound cargo container shipments; and the Coast Guard is responsible for, among other things, assessing the effectiveness of security measures in foreign ports and vessels that trade with the United States.

In performing its container security responsibilities, CBP has developed a layered, risk management approach⁴ that includes two security programs—the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) program. Under the CSI program, CBP places officials (targeters) at select foreign seaports to use intelligence and risk assessment information to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing WMD or other terrorist contraband. To aid in this process, CBP targeters use the Automated Targeting System (ATS)—an enforcement and decision support system that incorporates a set of rules to assess information provided by supply chain parties, such as importers—to identify high-risk shipments. C-TPAT is a voluntary program in which CBP officials work with private companies, referred to as partners, to review the security of their international supply chains and improve the security of their shipments to the United States. In return, C-TPAT partners receive various incentives to facilitate the flow of legitimate cargo, such as reduced scrutiny of their shipments.

³See, for example, the *National Strategy to Combat Weapons of Mass Destruction* (Washington, D.C.: December 2002), the *National Strategy for Maritime Security* (Washington, D.C.: September 2005), the *Strategy to Enhance International Supply Chain Security* (Washington, D.C.:2007), the *National Security Strategy* (May 2010), the *National Strategy for Counterterrorism* (Washington, D.C.: June 2011), and the *National Strategy to Combat Transnational Organized Crime* (Washington, D.C.: July 2011).

⁴Risk management is a strategy called for by federal law and presidential directive and is meant to help policy makers and program officials most effectively mitigate risk while allocating limited resources under conditions of uncertainty.

In addition to the CBP container security programs, the Coast Guard operates the International Port Security (IPS) program in which Coast Guard officials, in conjunction with foreign officials, visit and assess the implementation of security measures in foreign ports against established, international port security standards to help ensure the security of maritime commerce. In addition, CBP and the Coast Guard have separately entered into arrangements with foreign counterpart agencies to validate and mutually recognize each others' port security practices to more efficiently address maritime and supply chain security.

Since September 11, 2001, Congress has passed various laws to address concerns about the security of maritime cargo container shipments in the global supply chain. The Maritime Transportation Security Act of 2002 (MTSA)⁵ called for the establishment of a program to evaluate and certify secure systems of international transportation, including standards and procedures for screening and evaluating cargo containers prior to loading them onto vessels and for securing and monitoring cargo while in transit.⁶ One MTSA provision requires DHS to assess the effectiveness of the antiterrorism measures maintained at ports from which foreign vessels depart to the United States, or in any other port the Secretary of Homeland Security believes may pose a risk to international maritime commerce.⁷ The Secretary delegated this responsibility to the Coast Guard, which initiated IPS in 2004 to carry out this responsibility. To further address container security concerns, Congress passed, and the President signed, the Security and Accountability for Every (SAFE) Port Act in 2006, which included provisions that codified the CSI and C-TPAT programs.⁸

Given the importance of maritime transportation to the economy, the wide spectrum of security threats, and the constrained budget environment, you asked that we review DHS's maritime supply chain security programs. In particular, this report addresses the following questions:

⁵Pub. L. No. 107-295, 116 Stat. 2064.

⁶See 46 U.S.C. § 70116.

⁷46 U.S.C. § 70108.

⁸Pub. L. No. 109-347, 120 Stat. 1884.

-
- To what extent has DHS assessed the risks to the global supply chain associated with foreign ports and focused its maritime security programs to address those risks?
 - What actions has DHS taken to help ensure the efficiency and effectiveness of its maritime supply chain security programs?

To address the first question, we identified how DHS's components assess risk to the supply chain associated with foreign ports and countries.⁹ Specifically, we (1) gathered information on the criteria used to determine high-risk locations and the key stakeholders involved in developing any models or methodologies used to do so, (2) reviewed the methodology used to construct any models, and (3) determined the sufficiency of the models to identify high-risk locations. In particular, we reviewed the Coast Guard's IPS model for determining operational decisions, the methodology CBP used to select CSI ports, and the model developed by CBP and the Department of Energy (DOE) for potentially expanding cargo-scanning operations at foreign ports. To the extent possible, we compared the relative risk of foreign ports generated by these models with the location of CSI ports to determine the degree of correlation. As part of this process, we combined fiscal year 2012 data on the number of U.S.-bound shipments from foreign ports with data from the models and narrowed the list of ports based on a minimum of 1,000 U.S.-bound shipments—a step CBP took when developing its model in conjunction with DOE. We assessed the reliability of the models by interviewing staff responsible for development of the methodologies and the data and reviewing documentation related to the development, application, and reviews of the models. We concluded that the models and data were sufficiently reliable for the purposes of our review. In addition, we interviewed CBP, Coast Guard, DOE, and Department of State officials about the process used for identifying high-risk locations, the stakeholders involved in this process, and the status of these efforts. We compared this information with SAFE Port Act requirements, key elements for a risk management approach,¹⁰ and the principles laid out in

⁹For the purposes of this report, we used the following DHS definition of risk: the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. For example, risk is the expected consequences associated with a terrorist organization smuggling a WMD into a container at a foreign port and detonating that weapon in the United States.

¹⁰These key elements are contained in DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

the *National Strategy for Global Supply Chain Security*. We also reviewed our prior work on risk management practices and compared our analysis of CBP's actions with those practices.¹¹

To address the second question, we focused primarily on the CSI, C-TPAT, and IPS programs. Specifically, we analyzed CBP efforts to implement the fiscal year 2012 through 2017 CBP Office of Field Operations Strategic Plan and associated strategies in the CSI and C-TPAT Strategy Action Plans. We reviewed DHS documentation, such as the 2013 *DHS Annual Performance Report* and budget documents. Further, we reviewed CSI and C-TPAT performance measurement data and analyzed CSI staffing data from fiscal years 2009 through fiscal years 2012—the 4 most recent years for which data were available—to review the extent to which CSI staffing models have increased efficiency. In addition, we analyzed fiscal year 2012 Coast Guard foreign port visit data and foreign country risk data to determine the extent to which the Coast Guard uses the results of its risk assessments to help determine the amount of resources needed when visiting foreign countries' ports. We reviewed documentation related to the data sources, such as the 2013 *DHS Annual Performance Report*, and obtained written responses from knowledgeable agency officials regarding any issues with completeness, accuracy, and management of the data. We determined that these CBP and Coast Guard data were sufficiently reliable for the purposes of our review. We visited six geographically dispersed foreign countries that participate in the CSI program—two each in Latin America (Panama and Argentina), Asia (Japan and Singapore), and Europe (the Netherlands and England)—that also provided a range of coverage regarding (1) cargo container shipment risk levels, (2) volume of cargo containers shipped to the United States, (3) the proportion of transshipped containers,¹² and (4) participation in mutual recognition arrangements (MRA) with CBP or the Coast Guard.¹³ We interviewed DHS, Department

¹¹GAO, *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). Our prior work identified a risk management framework that we used to evaluate activities related to homeland security and combating terrorism.

¹²Transshipped containers are those that are unloaded from vessels at ports and are then reloaded to different vessels.

¹³Through MRAs with other partners, the security-related practices and programs taken by the customs or maritime security administration of one country are recognized and accepted by the administration of another. These arrangements are discussed in more detail later in this report.

of State, and foreign government officials in the countries we visited, and also met with other maritime supply chain stakeholders, such as officials from private industry and the World Customs Organization, to discuss implementation of DHS's maritime security programs, how these programs are integrated, the specific maritime security threats each program targets, and the impact of these programs on the security of U.S.-bound cargo container shipments. We worked with relevant officials at the U.S. embassies in the foreign countries we visited to help us determine which foreign government and industry officials to interview. The results from our visits to these six countries cannot be generalized; however, the visits provided us with first-hand observations on cargo security screening and targeting practices at the ports visited, and insights regarding how DHS implements its overseas maritime container security programs and the impact of these programs. In addition, we contacted officials from the seven partners that have signed an MRA with CBP and obtained the views of cognizant officials representing four of these partners. While the results of these meetings cannot be generalized to all seven MRA-signatory partners, they provided insights regarding the impact of the MRAs on DHS and other maritime security programs. Further, we interviewed the DHS Acting Director of Transportation & Cargo, Transborder Policy, to discuss implementation of the *National Strategy for Global Supply Chain Security* and how it affects maritime container security programs. We also interviewed Coast Guard officials responsible for the IPS program to discuss development and implementation of the Coast Guard IPS risk model and mutual recognition efforts.¹⁴

We conducted this performance audit from October 2012 to September 2013 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

¹⁴We also interviewed U.S. Immigration and Customs Enforcement officials regarding the Global Shield initiative to stem the illegal flow of precursor chemicals used in improvised explosive devices (IED), but we determined this program was outside the scope of this review because it is an international initiative, not a U.S. maritime security program. Global Shield is a World Customs Organization initiative in collaboration with the United Nations Office on Drugs and Crime and Interpol. Since its initiation in October 2010, more than 80 participating countries have monitored the import and export of 14 explosive precursor chemicals—identified as those most prevalently used in IEDs—around the world, in order to secure the global supply chain.

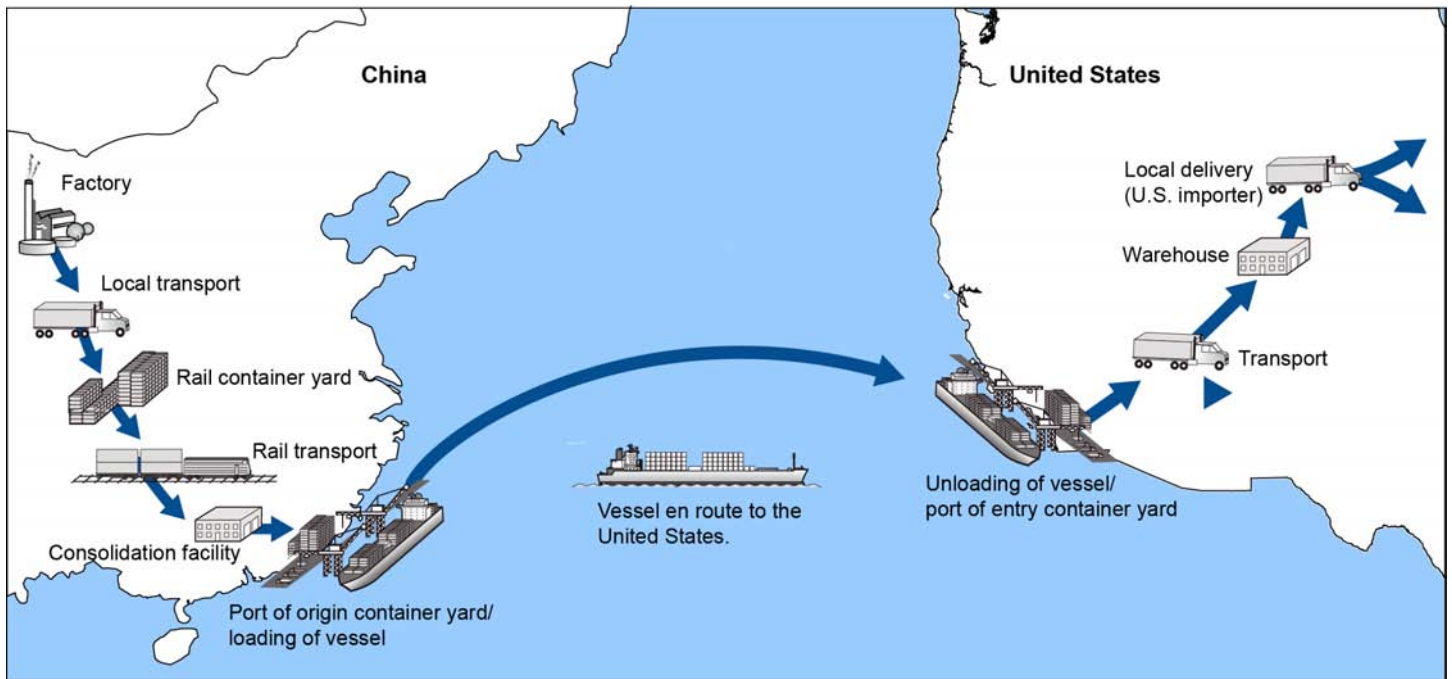
that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Vulnerabilities of Maritime Cargo Containers in the Global Supply Chain

Ports are critical gateways for the movement of commerce through the global supply chain. According to CBP data, in fiscal year 2012, about 11.5 million cargo container shipments arrived from more than 650 foreign ports—meaning roughly 31,000 maritime container shipments arrived each day that year. The facilities, vessels, and infrastructure within ports, and the cargo passing through them, all have vulnerabilities that terrorists could exploit. Every time responsibility for cargo in containers changes hands along the supply chain there is the potential for a security breach. While there have been no known incidents of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. Figure 1 illustrates the notional key points of transfer involved in the global supply chain—from the time that a container is loaded with goods at a foreign factory to its arrival at the U.S. seaport and ultimately the U.S. importer.

Figure 1: Illustrative Example of Key Points in the Global Supply Chain

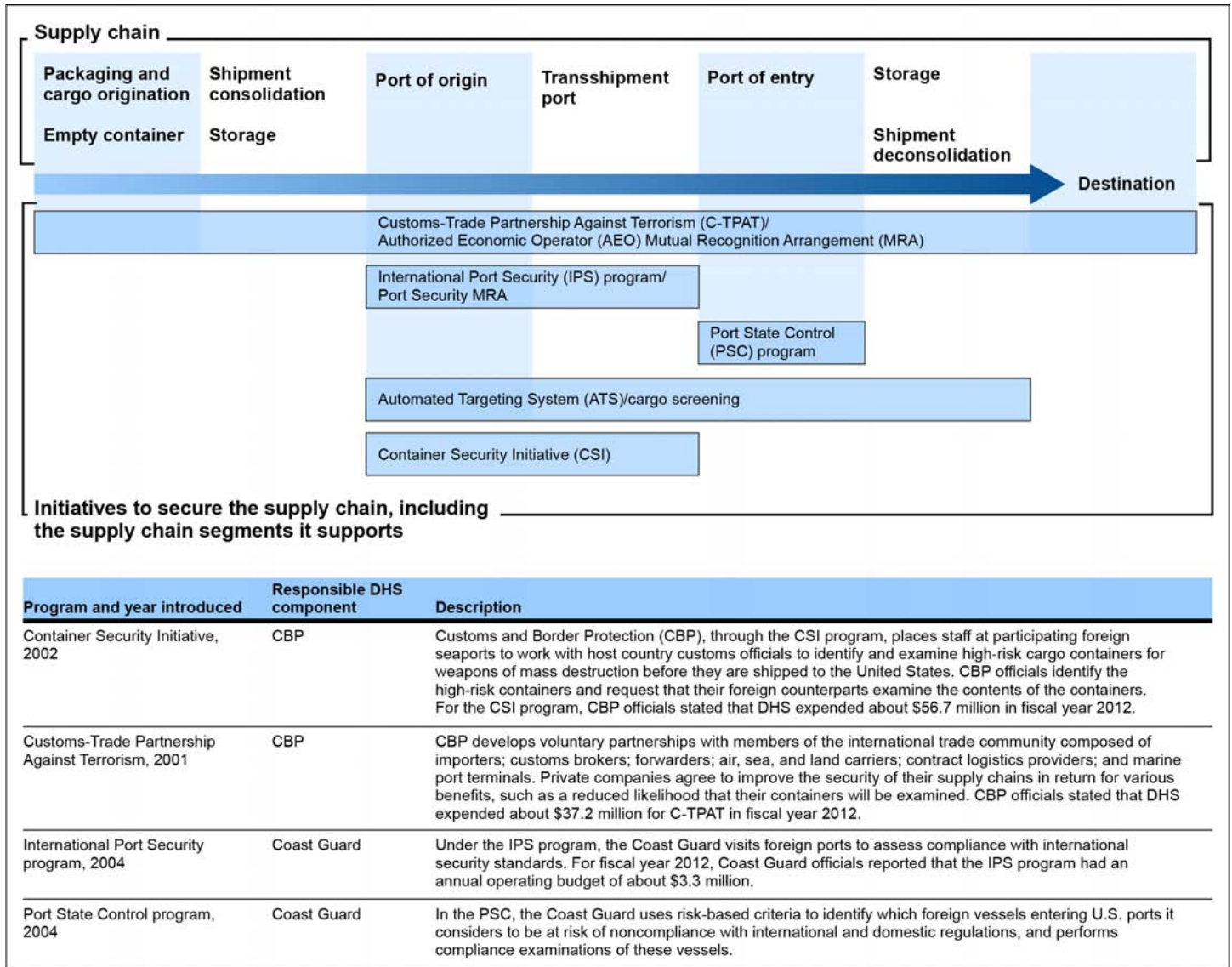


Source: GAO; Map Resources (map).

DHS Efforts to Secure the Global Supply Chain

DHS has taken steps to secure the global supply chain, including the cargo in oceangoing containers destined for the United States. DHS's strategy includes focusing security efforts beyond U.S. borders to target and examine high-risk cargo and vessels before they enter U.S. seaports. DHS's strategy is based on a layered approach of related programs that attempt to focus resources on potentially risky foreign ports, vessels, and cargo container shipments while allowing other cargo container shipments to proceed without unduly disrupting the flow of commerce into the United States. DHS's maritime security programs support the *National Strategy for Global Supply Chain Security*, which emphasizes risk management and coordinated engagement with key stakeholders who also have supply chain roles and responsibilities. Figure 2 shows DHS's key maritime security programs and the various segments in the global supply chain where these programs are focused.

Figure 2: Department of Homeland Security's (DHS) Key Maritime Security Programs



Source: GAO analysis of information provided by DHS.

Notes: AEOs include, for example, manufacturers, importers, exporters, brokers, ports, airports, terminal operators, warehouses, and distributors.

Through MRAs with other partners, the security-related practices and programs taken by the Customs or maritime security administration of one country are recognized and accepted by the administration of another.

ATS is a CBP enforcement and decision support system that incorporates a set of rules to assess information provided by supply chain parties, such as importers, to identify high risk shipments.

Container Security Initiative

CSI is a program that aims to identify and examine U.S.-bound cargo container shipments that could pose a high risk of concealing WMDs or other terrorist contraband by reviewing advanced cargo information about the shipments. As part of the CSI program, CBP officers are stationed at select foreign seaports to identify high-risk U.S.-bound container cargo shipments before they are loaded onto U.S.-bound vessels. As of July 2013, there were 58 CSI ports in 32 countries that, collectively, account for over 80 percent of the container shipments imported into the United States. In addition to the CSI ports where CBP placed targeters, CBP also entered into arrangements with Australia and New Zealand to remotely target U.S.-bound cargo container shipments from the United States.¹⁵ A complete listing of the countries that participate in the CSI program can be found in appendix I.

CBP officers stationed at foreign CSI ports are to conduct the following activities:

- **Target U.S.-bound container shipments.** As we previously reported, CBP targeters use ATS and other information to electronically review information about U.S.-bound shipments departing from the foreign port—a process CBP refers to as screening.¹⁶ CBP targeters review the ATS risk scores and additional information to identify high-risk shipments with a potential nexus to terrorism—a process referred to as targeting. The CBP targeters make a final determination about which containers are high risk and will be referred to host government officials for examination.
- **Request examinations of high-risk container shipments.** According to our work and updates provided by CBP officials, CBP

¹⁵According to CBP officials, CBP entered into arrangements with New Zealand (April 2006) and Australia (November 2011) to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58. Appendix I provides a complete listing of the 61 CSI ports.

¹⁶GAO, *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).

targeters work with host country government officials to mitigate high-risk container shipments.¹⁷ Actions may include resolving discrepancies in shipment information, scanning cargo containers' contents with radiation detection or imaging equipment (as shown in fig. 3), or conducting physical inspections of the containers' contents.

Figure 3: Panama Customs Examining a Container Using Imaging Equipment, Port of Balboa, Panama



Source: GAO.

Customs-Trade Partnership Against Terrorism

According to our prior work and updates provided by CBP officials, C-TPAT aims to secure the flow of goods bound for the United States by developing a voluntary public-private sector partnership with stakeholders of the international trade community.¹⁸ C-TPAT partners agree to adhere

¹⁷GAO-08-538.

¹⁸GAO-08-538.

to the program's eight established minimum security criteria in areas such as physical security, personnel security, and information technology. C-TPAT partners also agree to provide CBP with information regarding their security processes and procedures and allow CBP to validate or verify that these security measures are in place. In return, C-TPAT partners receive various incentives, such as reduced examinations based upon lower risk scores.

International Port Security Program

In addition to the CBP programs, the Coast Guard also has an internationally focused maritime security program, the IPS program. Under the IPS program, Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established International Ship and Port Facility Security (ISPS) Code standards.¹⁹ In addition, the Coast Guard collects and shares best practices with foreign countries and engages in efforts to help facilitate a comprehensive and consistent approach to maritime security in ports worldwide. Coast Guard officials reported that from its inception in April 2004 through June 2013, IPS program officials have visited port facilities in 151 countries and overseas protectorates engaged in maritime trade with the United States. According to its visits and the information provided by the foreign countries as part of those visits, the Coast Guard determines whether the countries have effectively implemented the ISPS Code and are maintaining effective security measures in their ports. If the Coast Guard finds that a country is not maintaining port security measures, the Coast Guard can impose conditions of entry on vessels arriving at the United States from that country.²⁰

Port State Control Program

The Coast Guard uses the results of the port risk assessments to help decide which foreign vessels to board or inspect through its Port State Control program, according to the U.S. Coast Guard *International Port*

¹⁹The IPS program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's antiterrorism measures in a port. The code was developed after the September 11, 2001, terrorist attacks to establish measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS Code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance-based; therefore, compliance can be achieved through a variety of security measures.

²⁰Conditions of entry may include restricting a vessel's movement within U.S. ports or requiring the vessel to take additional security measures, such as stationing guards at each access point of the ship when in a U.S. port.

Mutual Recognition Arrangements

*Security Program: Annual Report 2012.*²¹ While the Port State Control program does not directly affect container security, as part of this program, the Coast Guard uses risk-based criteria to identify which foreign vessels entering U.S. ports and waterways it considers to be at risk of noncompliance with international or domestic regulations, and performs compliance examinations of these vessels. The risk-based criteria include the vessel's management, the flag state that the vessel is registered under, the vessel's recognized security organization, and the vessel's security compliance history resulting from previous examinations.

Through mutual recognition arrangements with foreign partners, the security-related practices and programs taken by the Customs or maritime security administration of one partner are recognized and accepted by the administration of another.²² Both CBP and the Coast Guard have entered into such arrangements. For example, CBP can expand the reach of its supply chain security programs through MRAs. According to the World Customs Organization, mutual recognition allows Customs administrations to target high-risk shipments more effectively and expedite low-risk shipments by, for example, reducing redundant examinations.²³ The World Customs Organization distinguishes between mutual recognition of Customs controls and mutual recognition of authorized economic operator (AEO) programs:²⁴

- **Mutual recognition of Customs controls (Customs-to-Customs MRAs):** This is achieved when, for example, the Customs administrations of two countries have confidence in and accept each other's procedures for targeting and inspecting cargo shipped in containers.

²¹U.S. Coast Guard, *International Port Security Program: Annual Report 2012* (Washington, D.C.: March 31, 2012).

²²MRAs can be entered into with other countries as well as other governing bodies, such as the European Union. For the purposes of this report, the countries and governing bodies that enter into MRAs with the United States are considered "partners."

²³The World Customs Organization is an intergovernmental organization representing the customs administrations of 179 countries, which aims to enhance the effectiveness and efficiency of Customs administrations.

²⁴AEOs include, for example, manufacturers, importers, exporters, brokers, ports, airports, terminal operators, warehouses, and distributors.

-
- **Mutual recognition of AEO programs (AEO MRAs):** This occurs when Customs administrations agree to recognize one another's AEO programs and security features and to provide comparable benefits to members of the respective programs.

In the United States, C-TPAT is the designated AEO program and businesses participating in the program are AEOs. According to C-TPAT documentation, CBP has developed an AEO MRA process involving four phases: (1) a comparison of the program requirements to determine if the programs align on basic principles; (2) a pilot program of joint validation visits to determine if the programs align in basic practice; (3) the signing of an MRA; and (4) the development of mutual recognition operational procedures, primarily those associated with information sharing. MRAs are based on close working relationships between Customs administrations, which allow for the exchange of information, intelligence, and documents in an effort to assist countries in the prevention and investigation of Customs offenses.

The Coast Guard can also enter into MRAs that recognize international maritime security practices of other foreign governments. For example, the Coast Guard has a process in place to recognize the port inspection procedures of other countries.

One Hundred Percent Scanning Requirement

Although DHS's maritime security programs support the National Strategy for Global Supply Chain Security and the strategy's risk-informed security approach, the SAFE Port Act included requirements that pilot projects be established to test the feasibility of scanning 100 percent of U.S.-bound cargo containers at foreign ports.²⁵ Subsequently, 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 U.S.-bound cargo containers be scanned at foreign ports with both radiation

²⁵6 U.S.C. § 981. This pilot was called the Secure Freight Initiative. A similar cargo-scanning 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).

detection and nonintrusive inspection (imaging) equipment before being placed onto U.S.-bound vessels.²⁶

In June 2008 and in October 2009, we found that CBP faced numerous challenges in implementing the 100 percent scanning requirement at the pilot ports.²⁷ In October 2009, we recommended, among other things, that CBP conduct feasibility and cost-benefit analyses of implementing the 100 percent scanning requirement and provide the results to Congress along with any suggestions of cost-effective alternatives to implementing the 100 percent scanning requirement, as appropriate. CBP partially concurred with the recommendations but did not implement them. According to CBP officials, CBP does not plan to conduct these analyses related to achieving the 100 percent scanning requirement because the pilot project has been reduced in scope and currently there are no funds to conduct such analyses. In February 2012, we reported that the scanning challenges continued, and CBP achieved 100 percent scanning of U.S.-bound cargo containers at only one foreign pilot port where it was being attempted—Port Qasim, Pakistan.²⁸ In May 2012, the Secretary of Homeland Security announced a 2-year extension of the deadline—until July 2014—for implementing the requirement that cargo containers not enter the United States unless they are scanned at foreign ports prior to

²⁶Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)). Radiation detection equipment detects radiation being emitted from a container, and through a nonintrusive image scan, CBP can identify anomalies in a container's image that could, among other things, indicate the presence of dense material used to shield radioactive material.

²⁷GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, [GAO-08-533T](#) (Washington, D.C.: June 12, 2008), and *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).

²⁸GAO, *Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning*, [GAO-12-422T](#) (Washington, D.C.: Feb. 7, 2012).

being loaded on vessels.²⁹ In its report to Congress that same month, DHS stated that it recognizes the need to proceed with its container security programs in a manner that maximizes the security of maritime cargo and facilitates its movement. DHS added that it plans to continue working with other federal agencies and international partners to develop technology and enhance risk management processes, in addition to continuing its existing container security programs.³⁰ According to the January 2013 *National Strategy for Global Supply Chain Security Implementation Update*, DHS is working to identify potential alternatives to 100 percent scanning, and a senior DHS official told us that DHS's layered security strategy will be a key component of the alternative.³¹

DHS Has Developed Models to Assess Foreign Port Risks, but CBP Has Not Assessed Whether Its CSI Locations Remain Valid

The Coast Guard and CBP, DHS components with maritime security responsibilities, have developed models to assess the risks of foreign ports and the cargo carried by vessels from these ports. The Coast Guard uses the model it developed to inform operational decisions for its IPS program and updates its assessment annually. In contrast, in 2009, CBP developed a risk model to begin the process of expanding its efforts to scan 100 percent of U.S.-bound container shipments, but the model was never implemented. As a result, it does not know whether the ports included in CSI remain valid.

²⁹The 9/11 Act scanning provision includes possible extensions for containers loaded at 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 the following: (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 affect trade capacity and the flow of cargo. See 6 U.S.C. § 982(b)(4). The 9/11 Act also requires DHS to submit a report to Congress on whether it expects to seek to renew the extension 1 year after it takes effect. See *id.* § 982(b)(7). As of July 2013, DHS has not provided this report to Congress.

³⁰DHS, *Scanning of Maritime Cargo Containers: Fiscal Year 2012 Report to Congress* (Washington, D.C.: May 3, 2012).

³¹The White House, *National Strategy for Global Supply Chain Security Implementation Update* (Washington, D.C.: January 2013).

The Coast Guard Has Developed a Model to Regularly Assess Risks of Foreign Ports and Inform Operational Decisions

The Coast Guard has developed a risk-informed model as part of its IPS program to regularly assess the potential threat foreign ports pose to the maritime supply chain and make operational decisions regarding foreign ports' security measures. According to the 2012 IPS program annual report, this risk model includes four components, summarized below, that help the Coast Guard focus IPS program resources.

Country threat. The Coast Guard uses security and commerce data as well as measures on government decision making, such as the prevalence of corruption, to assess the likelihood of terrorists using a foreign port to import WMDs or other contraband into the United States. In particular, the Coast Guard relies on CBP trade information, the U.S. Department of State's Security Environment Threat List, World Bank reports, and other data to determine whether countries represent a normal, medium, or high security risk.

Foreign port assessment. MTSA, as amended by the SAFE Port Act, requires the Coast Guard to reassess countries' ports every 3 years, and during these visits, IPS officials use two data checklists, one that assesses government performance and one that assesses facilities' performance.³² The government performance checklist measures how well a government gathers and assesses information on security threats, and reviews and approves port facility security plans, among other things. The facilities performance checklist measures port security measures implemented to prevent unauthorized cargo and people from entering the port. Such security measures include, for example, perimeter security and access procedures for port facility employees and visitors.

Country responsiveness. The IPS model includes measures of the political, economic, and social conditions in a country to help determine whether countries are likely to efficiently utilize Coast Guard assistance. The model incorporates information on corruption, inflation, and "people measures," such as infant mortality rates and literacy rates.

Country wealth. The IPS model includes a measure of national income to determine if the country can afford to maintain security measures on its own or whether it is likely to require foreign assistance.

³²46 U.S.C. § 70108(d).

According to the 2012 IPS program annual report, the Coast Guard combines these components into a single risk model and uses the results to make informed decisions on how to engage each country with the IPS program, including (1) how often to visit ports, (2) how many staff to assign to a particular visit, and (3) whether the country requires assistance. Specifically, the Coast Guard visits foreign ports in higher-risk countries more frequently (and with more IPS officials) than in ports in lower-risk countries, which we discuss later in this report. In addition, the IPS annual report states that the Coast Guard uses the country threat component of the IPS risk model to help determine which foreign vessels to board as part of its Port State Control program. The Coast Guard updates its risk model annually. While elements of the Coast Guard's risk model could be used to inform maritime container security efforts, there are limits regarding how it can be applied to maritime supply chain security because the IPS program is focused on assessing port security. Unlike the CBP risk model described below, the Coast Guard's model is not designed to assess the risk of maritime cargo shipments imported from foreign ports (e.g., transshipped cargo).

CBP Considered Risk in Establishing Some CSI Ports, but Has Not Assessed Whether CSI Currently Covers the Riskiest Ports

CBP Selected Initial CSI Ports Largely on the Basis of Volume and Used More Risk Factors when Expanding CSI Locations

In 2002, CBP selected the initial 23 CSI ports largely on the basis of the volume of U.S.-bound container cargo, but increased the number of risk factors in selecting additional ports as it expanded the CSI program beginning in 2003.³³ Specifically, according to CBP documentation, volume was a key criterion for assessing which foreign ports represented the greatest threat to the United States. Figure 4 shows the large number of containers shipped through the Port of Singapore, one of the original CSI ports.

³³According to CBP officials, because of logistical factors such as the time necessary for negotiations with host governments and staffing CSI teams in foreign countries, initial CSI ports selected on the basis of volume sometimes did not begin operations until the expansion of CSI was under way.

Figure 4: Partial View of the Port of Singapore



Source: GAO.

After selecting these initial 23 ports, CBP subsequently added 35 ports to the CSI program from 2003 through 2007 on the basis of additional criteria, such as strategic threat factors and diplomatic or political considerations. Through these expansion efforts, in 2007 CBP reached its goal of staffing 58 CSI ports that, collectively, cover over 80 percent of U.S.-bound container shipments.³⁴ We reported in 2008 that CBP did not have plans to add other ports to the CSI program because, according to CBP, the costs associated with expanding the program would outweigh the potential benefits.³⁵

³⁴According to CBP officials, CBP entered into arrangements with New Zealand (April 2006) and Australia (November 2011) to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58.

³⁵GAO, *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).

CBP Developed a Risk Model for Expanding Container Security Efforts at High-Risk Ports, but It Was Never Implemented

In 2009, CBP developed a risk model in conjunction with DOE to begin the process of expanding its efforts to scan 100 percent of U.S.-bound container shipments for a related program, but the model was never implemented. In particular, in April 2009, the Secretary of Homeland Security approved the “strategic trade corridor strategy” as an approach to expanding CBP’s efforts to scan U.S.-bound container cargo beyond the original pilot locations.³⁶ As part of this expansion effort, CBP developed a model—assisted by DOE—to rank potential foreign ports on the basis of risks associated with countries and maritime commerce, as well as the number and percentage of high-risk, U.S.-bound shipments processed. Specifically, DOE provided the country threat and shipping lane information from the model it used to identify and prioritize foreign ports for participation in the Megaports Initiative,³⁷ and CBP provided the high-risk shipment data from ATS. CBP and DOE completed their initial analyses in February 2009, which identified 356 potential expansion ports ranked by risk, and CBP narrowed the list down to 187 ports by considering only ports that had at least 1,000 shipments per year to the United States. CBP collaborated with DOE, the Department of State, and the intelligence community to prioritize 22 ports for expansion of 100 percent scanning efforts on the basis of such factors as the model’s risk ranking and the volume of U.S.-bound cargo container shipments. CBP ultimately did not pursue this strategy, given cargo security program budget cuts and the Secretary of Homeland Security’s decision to extend the deadline for 100 percent scanning until July 2014.

The results of the 2009 strategic trade corridor prioritization model show that the CSI program is operating at some of the riskiest foreign ports, but it also operates at ports that are less risky. Since the model focused on U.S.-bound maritime containerized cargo, its results could be used as a proxy measure to assess whether CSI ports coincide with those foreign locations that pose the greatest risk to the global supply chain. We

³⁶The original pilot locations were Busan, South Korea; Puerto Cortes, Honduras; Qasim, Pakistan, Salalah, Oman; Southampton, United Kingdom; and Hong Kong.

³⁷DOE established the Megaports Initiative in 2003 to deter, detect, and interdict nuclear or other radiological materials smuggled through foreign ports. The initiative funds the installation of radiation detection equipment at select ports overseas and trains host country personnel to use this equipment to scan cargo containers entering and leaving these ports—regardless of destination. The Megaports Initiative was intended to complement the CSI program. See GAO, *Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenge*, [GAO-13-37](#) (Washington, D.C.: Oct. 31, 2012).

combined the risk rankings for the 356 ports in the 2009 model with fiscal year 2012 U.S.-bound shipment data and excluded ports with fewer than 1,000 U.S.-bound shipments per year, which narrowed the list to 138 ports.³⁸ Comparing the CSI ports with the results shows that CSI did not have a presence at about half of the ports CBP considered higher risk, and about one-fifth of the existing CSI ports were at lower-risk locations. Specifically, of the 61 current CSI ports, 57 had at least 1,000 U.S.-bound shipments in fiscal year 2012. Of these 57 CSI ports, 27 were within the top 50 riskiest ports, 18 ports were between the 51st and 100th riskiest ports, and 12 ports were not among the top 100 riskiest ports. Of the remaining 4 CSI ports, 3 had fewer than 1,000 U.S.-bound shipments and 1 port was not ranked in the 2009 risk model. According to CBP officials, CBP has not established CSI locations in 15 of the top 50 riskiest ports either because host governments have not been cooperative regarding CBP cargo examination requests or CBP was not able to negotiate an arrangement with host governments to establish CSI operations, as discussed below.

CBP officials stated that factors have changed since the model was developed in 2009, and they do not consider all of the same ports to be high risk at this time. For example, one potential expansion port the model classified as higher risk in 2009 now ships fewer containers to the United States, and CBP officials reported that they would not currently consider including this port in the CSI program. Further, according to CBP's fiscal year 2012 budget submission, CBP considered closing several CSI ports while maintaining CSI operations in strategically important ports. Given this information, and the fact that the number and location of CSI ports has generally not changed since 2009, the CSI program's current locations may not be in alignment with the highest-risk ports.

Because the CSI program depends on the willingness of sovereign host countries to participate in the program, there are challenges to implementing CSI and CBP efforts to negotiate with other countries to

³⁸Fiscal year 2012 data were not available for 67 of the 356 ports in the 2009 model and were excluded from the analysis. However, only 3 of these ports were ranked among the top 100 riskiest ports. In addition, 3 CSI ports had fewer than 1,000 U.S.-bound shipments in fiscal year 2012 and were therefore not included in the analysis. We reached 138 ports with at least 1,000 U.S.-bound shipments instead of the 187 determined by CBP because we used fiscal year 2012 shipment data instead of the data included in the 2009 risk model.

CBP Has Not Assessed the Risks of Foreign Ports that Ship Cargo to the United States since 2005

expand the CSI program, and these efforts have not always been successful. CBP and the Department of State point to challenges in implementing CSI in high-risk countries, such as CBP officer safety, funding concerns, and the willingness of host country governments to facilitate requested cargo examinations of U.S.-bound shipments. CBP officials stated that CBP is not pursuing the strategic trade corridor strategy, but they noted that since the beginning of the CSI program, CBP has made efforts to negotiate to establish CSI ports within four countries that have ports representing potential significant risks. These efforts were not successful in three countries for political reasons. For example, the legislature in one of these countries did not approve the placement of CSI in its country. However, according to CBP officials, CBP has signed a declaration of principles to place CSI in an additional foreign country and estimates that CSI will be operational within this country by the end of fiscal year 2014.

CBP has not assessed the risk of foreign ports that ship cargo to the United States for its CSI program since completing the CSI expansion analysis in 2005. CBP officials stated they have not performed any such risk assessments since 2005 because CBP does not have any specific expansion plans for the CSI program. However, our work indicates that CBP may expand CSI. In particular, CBP's fiscal year 2013 and 2014 budget requests noted that CBP may expand CSI in the future to additional countries of strategic interest, if feasible; and CBP officials told us that CBP is finalizing negotiations with a foreign government to expand CSI to an additional port, as discussed above.

We acknowledge that CBP may face challenges in including foreign ports that ship the riskiest cargo to the United States in its CSI program, but expanding CSI without assessing the security risk posed by foreign ports is contrary to agency policy. In particular, according to the CSI Statement of Policy and Intent signed by the CBP Commissioner in April 2011, CBP is to prioritize CSI expansion locations in accordance with the *National Strategy for Global Supply Chain Security*, which states that the federal government should take a risk-informed approach to secure the global supply chain. Further, the SAFE Port Act provides that DHS/CBP is to assess the costs, benefits, and other factors associated with designation of a CSI port, including the level of risk for the potential compromise of containers by terrorists, or other threats as determined by DHS; the volume of cargo being imported to the United States directly from, or

being transshipped through, the foreign seaport; and the results of the Coast Guard's IPS assessments.³⁹

In addition to not completing a risk assessment to help inform potential CSI expansion, CBP has also not assessed the risk of its current CSI ports—some of which have participated in CSI for more than a decade—to determine if they remain valid on the basis of risk. CBP officials stated that they have not conducted such an assessment because a couple of factors make it difficult to close CSI ports and reallocate resources to prospective new CSI ports. In particular, the officials stated that (1) removing CSI from a country might negatively affect political relations with the host government, and (2) uncertain CSI funding in future years could make it difficult for CBP to make plans to close lower-risk CSI ports and open new CSI ports at higher-risk locations. Specifically, CBP officials estimate that it could take about 1 year to close a CSI port and 2 years or more to open a new port, and, given budget uncertainties, CBP has not pursued such efforts.

It is unclear if the political and cost challenges CBP officials identified would affect any reallocation of CSI resources to prospective new CSI ports, but these challenges do not preclude CBP from assessing the risk of its current CSI locations. Regarding the impact of changes to the CSI program on political relations, CBP officials stated they routinely speak to host government officials during CSI evaluations about how to strengthen the program, but these officials said that the discussions have not specifically included the impact on relations with the host government of removing lower-risk ports from the CSI program. Further, it is unclear if reallocating resources from current CSI ports to higher-risk ports would ultimately increase costs because some costs—such as staffing costs and office space leases—could be lower in some of the new locations than costs in the lower-risk ports it would be leaving. Moreover, the DHS *National Infrastructure Protection Plan*⁴⁰ and our *Risk Management Framework*⁴¹ state that risk assessments, the effectiveness of measures to deal with risks, and the costs of those measures are to inform decisions. Our framework also states that agencies should periodically

³⁹9 U.S.C. § 945(b).

⁴⁰DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

⁴¹See [GAO-06-91](#).

evaluate the cost-effectiveness of their programs and that mechanisms for altering a program should be in place based on current risk data. In addition, the DHS *National Infrastructure Protection Plan* states that effective protective programs seek to use resources efficiently by focusing on actions that offer the greatest mitigation of risk for any given expenditure. The plan also states that risk management includes a feedback loop that continually incorporates new information, such as changing threats or the effect of actions taken to reduce or eliminate identified threats, vulnerabilities, or consequences.

We recognize that it may not be possible to include all the higher-risk ports in CSI because CSI requires the cooperation of sovereign foreign governments and because of concerns regarding the security of U.S. personnel that may be staffed in those countries. Nevertheless, given that CBP is no longer pursuing implementation of 100 percent scanning, it is important that CBP apply the risk management principles discussed above to CSI—a risk-informed program—to more effectively mitigate the threat of high-risk cargo before it is shipped to the United States. Periodically assessing the risk level of cargo shipped from foreign ports and using the results of these risk assessments to inform the CSI locations would help ensure that CBP is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing WMDs or other terrorist contraband into the United States through the maritime supply chain.

DHS Has Taken Steps to Improve the Efficiency and Effectiveness of Its Maritime Container Security Programs, but Faces Constraints

DHS, through the Coast Guard and CBP, has taken a number of steps to improve the efficiency and effectiveness of its maritime security programs to reduce global supply chain risks. In this regard, the Coast Guard's actions have primarily been focused on the IPS program. CBP has continued its efforts to expand or refine its C-TPAT and CSI programs, but faces host country political and legal constraints.

The Coast Guard Has Worked to Reduce Global Supply Chain Risks by More Efficiently and Effectively Using IPS Resources

The Coast Guard has worked to use resources more effectively and reduce risks at foreign ports and from U.S.-bound vessels through its IPS program by implementing a risk-informed model that prioritizes the countries to visit and provide with assistance. When the Coast Guard first implemented the IPS program in 2004, it was required by MTSA to assess the effectiveness of antiterrorism measures maintained in ports where U.S. vessels call or from which vessels depart for the United States. As a result, the Coast Guard focused on completing initial visits of foreign ports to determine ISPS Code compliance, but did not have a methodology to prioritize follow-up visits and help countries increase their level of port security. To accomplish these goals, in 2005, the Coast Guard began developing its IPS risk model to assess the risks of foreign ports and prioritize assistance, which it fully integrated into IPS operations in 2011. The Coast Guard classifies countries as normal, medium, or high security risks and completes port security checklists during foreign port visits.

The Coast Guard Uses Its Risk Assessments to Manage Port Visits and Allocate Foreign Assistance

According to the 2012 IPS program annual report, the Coast Guard uses the results of its risk assessments to help determine the amount of resources needed to visit foreign countries' ports, board foreign vessels, and track port security improvements. Specifically, the Coast Guard uses the risk model results to more efficiently and effectively allocate resources to help ensure that visits to foreign ports in higher-risk countries occur more frequently (and with more IPS officials) than to ports in lower-risk countries.⁴² Table 1 provides information on Coast Guard IPS program visits, by country risk level, for fiscal year 2012.

⁴²Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established ISPS Code standards.

Table 1: Coast Guard International Port Security Program Visits, by Country Risk Level, for Fiscal Year 2012

Foreign country risk level	Number of foreign countries visited ^a	Average number of staff days per visit ^b	Average cost per visit ^c
Normal risk	13	14	\$9,926
Medium risk	18	29	\$27,193
High risk	23	37	\$38,214

Source: GAO analysis of Coast Guard data.

^aThrough the International Port Security program, the Coast Guard makes a determination of country, not port, risk level.

^bStaff days are cumulative for all Coast Guard staff involved in foreign port visits. According to Coast Guard officials, many visits were the result of multiple trips and often included different staff on the team.

^cAccording to Coast Guard officials, costs reflect travel and per diem costs as well as any funds provided to the U.S. embassy for translators, additional security, and in-country flights, among other things. They do not reflect any salary or overhead costs.

IPS program officials we met with that are responsible for assessing ports in Africa and Southeast Asia stated that this risk-informed approach helps the Coast Guard more efficiently use its resources. Further, the IPS program has enabled the Coast Guard to measure foreign countries' port security based on improvements its officials observe when completing foreign port visits. According to the 2012 IPS program annual report, port assessment scores have improved worldwide since the Coast Guard initiated the IPS program in 2004. The Coast Guard attributes this success, in part, to implementation of the IPS risk model.

According to the 2012 IPS program annual report, the Coast Guard also uses the results of the IPS model to allocate foreign assistance. The risk model includes (1) country threat information; (2) port visit results; (3) a determination of which countries are most likely to benefit from assistance to improve port security, such as port security training; and (4) the individual country's ability to best use assistance funds and sustain security efforts, as discussed earlier in this report. The 2012 report also states that Coast Guard officials are to use this information to direct resources to those foreign countries where they believe the return on investment will be greatest. Further, this report states that the Coast Guard uses the results of the IPS risk model to help determine which foreign vessels to board as part of its Port State Control program. The risk-based screening tool the Coast Guard uses to select vessels to board assigns point values to various risk factors, such as country threat data

MRAs May Allow the Coast Guard to Allocate Resources More Efficiently

from the IPS risk model. In addition, the Coast Guard boards foreign vessels that have recently stopped in higher-risk ports (i.e., countries that have not substantially implemented the ISPS Code).

In addition to prioritizing resources through its IPS risk model, the Coast Guard has worked with foreign governments to mutually recognize each other's maritime security programs, which can more efficiently use IPS resources and reduce risks. For example, in September 2012, the Coast Guard signed a memorandum of understanding (MOU) with the European Union that establishes a process for mutually recognizing security inspections of each other's ports.⁴³ The European Union has developed 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 European Union inspections of member states' ports that result in reports that (1) identify any nonconformities with the regulations and (2) make recommendations to address any nonconformities.

Under the MOU procedures, the Coast Guard recognizes a successful European Union inspection of its member states' ports in the same manner as it would recognize a successful country visit by Coast Guard IPS inspectors. Coast Guard IPS officials stated that they have collaborated with their European counterparts to develop standard operating procedures for these port inspections and they were used in a recent joint inspection of a container facility in Felixstowe, the United Kingdom. According to DHS documents and Coast Guard IPS officials in Europe, by signing this MOU, the Coast Guard plans to reassign some IPS officials from Europe to Africa, where certain countries are having more difficulties in implementing effective antiterrorism measures in their ports. Coast Guard IPS officials reported, however, that a trade-off of signing the MOU is that its IPS officials will not have the same opportunities to have face-to-face interactions and share port security information and practices directly with their European Union counterparts as in the past. Despite this trade-off, the Coast Guard IPS officials stated that entering into such arrangements increases efficiencies and noted that they intend to negotiate additional MOUs with other foreign governments that have strong port inspection programs.

⁴³According to DHS officials, the European Union characterizes its port visits as "inspections."

CBP Has Worked to More Efficiently Use Resources and Expand Its C-TPAT Membership

CBP Has Taken Steps to More Efficiently Use Resources by Negotiating MRAs

CBP has worked with foreign partners to mutually recognize each other's AEO programs to more efficiently use resources while continuing to reduce risks to the global supply chain. According to the World Customs Organization, as of June 2013, there were 25 AEO programs worldwide, other than C-TPAT, with which CBP could enter into an MRA. As part of the evaluation of a foreign partner's capacity for entering into an MRA, CBP conducts joint validations with the other partner to ensure that a partner's AEO program has security standards that are equivalent to those required by the C-TPAT program. CBP officials stated that CBP does not pursue mutual recognition with a Customs administration that does not have an equivalent AEO program in place because doing so could compromise the security of U.S.-bound container shipments. As of July 2013, CBP had signed MRAs with seven foreign Customs administrations—New Zealand in 2007, Canada and Jordan in 2008, Japan in 2009, the Republic of (South) Korea in 2010, and the European Union and the Taipei Economic and Cultural Representative Office (Taiwan) in 2012—and is in the process of negotiating MRAs with five other partners. CBP officials stated that they expect to complete MRA negotiations with one partner by the end of fiscal year 2013 and that they generally complete one or two MRAs each year.

To help foreign countries establish AEO programs, CBP officials stated that the C-TPAT program provides training and technical assistance for foreign Customs agencies that request technical assistance. As of April 2013, CBP officials reported that C-TPAT has provided assistance to about 70 foreign countries and noted that this assistance improves global supply chain security. Further, CBP officials told us that the goal of this assistance is to establish AEO-MRAs with foreign Customs agencies as a means to increase efficiencies in supply chain security efforts. According to CBP officials, by relying on MRA partners to validate supply chain security procedures overseas, CBP is able to operate more efficiently by reducing the costs associated with conducting security validations. For example, in 2010, CBP completed a study on AEO validation visits conducted on its behalf in Japan and Canada by the respective host governments. On the basis of cost data from prior validation visits, CBP estimates the C-TPAT program saved over \$290,000 and over 1,500 staff hours by accepting the 90 validations completed by the Japanese and

Canadian governments during 2009 and 2010.⁴⁴ Further, according to CBP officials, mutual recognition leads to a common understanding of global supply chain security standards, resulting in greater program efficiency and a streamlined validation process by reducing the number of redundant validations. As a result, mutual recognition enables CBP to focus its resources on higher-risk supply chains. CBP officials also stated that AEO program officials are in a better position to conduct validations of companies within their respective AEO programs because these officials are proficient in the local language and are more familiar with the companies' supply chains.

MRAs can increase efficiencies in the C-TPAT program, but CBP faces challenges in implementing MRAs. According to C-TPAT data, since 2009, CBP has accepted over 480 validations conducted by staff from foreign governments that have signed MRAs with the United States. Further, these data show that the number of validations conducted by MRA partners has increased significantly each year from 2009 (26) through 2012 (285), and CBP officials stated that they expect the number of validations to continue to increase because the European Union and Taiwan—two of the United States' largest trading partners—are expected to conduct more validations in 2013. While MRAs have resulted in increased efficiencies, CBP and foreign government officials we met with identified challenges in implementing MRAs. For example, CBP and foreign government officials we met with stated that exchanging data across information technology systems can be difficult, and government officials from one foreign partner stated that differences in privacy laws between partners can create additional hurdles to information sharing. As a result, it may take time for the benefits to be evident to the AEO partners. Specifically, private sector trade officials in one country we visited reported that they had not yet realized the benefits of the MRA through reduced inspections of their shipments at U.S. ports. In addition, World Customs Organization officials we met with said that it may be difficult to document the benefits of MRAs through reduced inspections because U.S. agencies other than CBP also have their own inspection procedures for imported cargo that are not part of any MRA. For example, according to CBP, the Food and Drug Administration has its own inspection process. As a result, MRA participants' shipments could still be

⁴⁴The study did not account for any costs associated with negotiating the MRAs. C-TPAT has not conducted any cost studies related to the MRAs with Jordan, New Zealand, Taiwan, South Korea, or the European Union.

slowed. According to CBP officials, CBP is working with other federal agencies to harmonize the inspection process at ports of entry and accelerate inspection decision making to address this issue.

CBP has entered into AEO-MRAs with other partners, but does not have plans to negotiate Customs-to-Customs MRAs. Under a Customs-to-Customs MRA, joint activities, such as identifying cargo for examination, would not require the placement of CBP targeters in foreign ports under programs like CSI. CBP officials said they do not have plans to negotiate Customs-to-Customs MRAs because they are much more difficult to achieve than AEO-MRAs, in part, because of the difficulties in ensuring Customs practices are applied consistently. For example, CBP officials said that Customs-to-Customs MRAs would need to include a broader validation of foreign Customs administrations' practices. World Customs Organization officials we met with concurred that achieving mutual recognition of Customs controls is difficult and noted that the focus of Customs administrations worldwide is on negotiating AEO-MRAs rather than Customs-to-Customs MRAs.

CBP Has Made Efforts to Improve Efficiency and Effectiveness by Increasing C-TPAT Membership

CBP has also made efforts to improve the efficiency and effectiveness of its C-TPAT program—and thus the security of the global supply chain—by increasing the number and category of C-TPAT members. For example, CBP has increased C-TPAT membership by conducting outreach events to increase awareness of the C-TPAT program and incentives. From fiscal years 2008 through 2012, the number of C-TPAT members increased by 15 percent—from 8,882 to 10,425. According to the 2013 DHS Annual Performance Report, as of fiscal year 2012, C-TPAT members account for more than 50 percent of all U.S. cargo imports (by value), which exceeds CBP's performance target goal of 45 percent. Further, as part of C-TPAT's membership expansion efforts, the program is considering adding two supply chain sectors—exporters and distribution centers.⁴⁵ CBP officials reported that C-TPAT selected these sectors because they can have a direct impact in securing the global supply chain. Moreover, according to the 2012 C-TPAT Strategy Action Plan, increased membership in the C-TPAT program could allow U.S. ports of entry to operate more efficiently because CBP officials at these

⁴⁵As of July 2013, C-TPAT membership is spread over 10 different supply chain sectors, such as importers and port operators.

Staffing Challenges and
Members' Compliance with
Security Requirements Limit
CBP Efforts to Improve C-
TPAT Effectiveness

ports would be able to focus CBP's targeting and inspection resources on a smaller percentage of high-risk shipments.

Although expansion of C-TPAT membership should increase program efficiencies systemwide, CBP faces challenges in increasing C-TPAT effectiveness because of staffing challenges. In particular, while the C-TPAT program has continued to expand in size and scope in recent years, staffing within the program has decreased. Specifically, according to CBP officials, as of July 2013, the C-TPAT program had 155 staff, down from a peak of 196 staff in January 2011. CBP plans to take several steps to address this staffing challenge. For example, CBP officials reported that as of July 2013, C-TPAT is working with CBP's Office of Human Resources to hire 11 additional Supply Chain Security Specialists.⁴⁶ Furthermore, according to fiscal year 2014 CBP budget documentation, CBP plans to extend the C-TPAT revalidation cycle to once every 4 years as mandated by the SAFE Port Act rather than accelerating the revalidation schedule to once every 3 years as CBP had previously done. Moreover, C-TPAT officials reported that CBP anticipates a reduction in foreign validation visits by its specialists through the implementation of MRAs.

An additional challenge to C-TPAT program effectiveness is that C-TPAT partners' compliance rates with program security requirements decreased from almost 100 percent in fiscal year 2008 to about 95 percent in fiscal year 2012. According to CBP documentation, the overall compliance rate decreased after CBP strengthened C-TPAT security criteria and increased program oversight. CBP reported that C-TPAT is working with C-TPAT partners to explain the enhanced security criteria to ensure they understand the validation requirements. CBP officials said that they expect this will lead to improvements in C-TPAT partners' compliance with the security requirements.

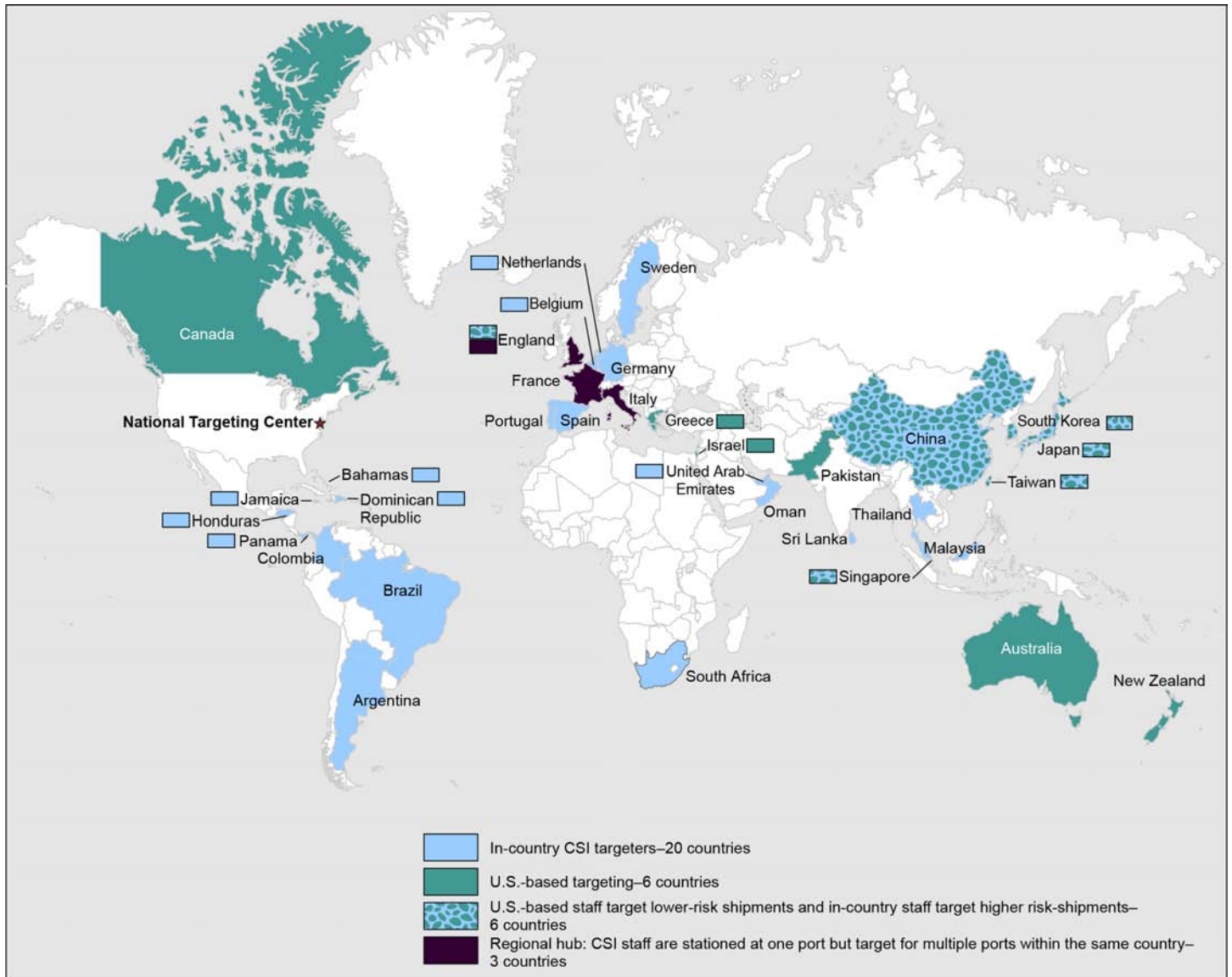
⁴⁶Supply Chain Security Specialists are responsible for responding to the needs of C-TPAT partners, as well as conducting training and outreach efforts with local law enforcement, CBP components, and other entities.

CBP Revised CSI in Response to Budget Cuts, but Efficiencies and Effectiveness Are Limited by Political and Legal Factors

CBP Revised CSI Targeting Approaches to Address Budget Cuts

As a result of reduced program budgets in recent years, CBP has implemented CSI changes to take advantage of improvements in technology and more efficiently use its CSI targeters, but efficiencies are limited by host country political and legal factors. Specifically, CSI program expenditures declined by more than \$50 million from fiscal years 2008 through 2012, and this cut led to changes in how CBP has staffed its CSI ports. As shown in figure 5, CBP employs a variety of approaches in targeting and examining U.S.-bound containerized cargo imported from CSI countries. These targeting approaches are explained below.

Figure 5: Map Showing the Variety of Targeting Approaches Customs and Border Protection Uses in Container Security Initiative Countries as of July 2013



Notes: Targeting refers to the review of shipment data and additional information by CBP officials to identify high-risk shipments with a potential nexus to terrorism.

CSI ports in England utilize both the regional hub and a mixture of in-country and U.S.-based targeting approaches.

CBP coordinates targeting of U.S.-bound cargo container shipments in 34 countries that covers 61 foreign ports.

National Targeting Center-Cargo (NTC-C) support. In April 2005, we recommended that CBP revise the CSI targeting approach to consider what functions need to be performed at CSI ports and what functions can be performed in the United States.⁴⁷ CBP agreed with this recommendation and, in January 2009, began transferring some CSI staff from overseas ports to perform targeting remotely from the NTC-C. According to CBP officials, NTC-C staff are less costly than overseas staff.⁴⁸ Under this revised targeting approach, NTC-C targeters review U.S.-bound shipments from foreign ports in 6 CSI countries. For those shipments that NTC-C targeters determine to be high risk or suspect, NTC-C targeters request that host government Customs officials complete examinations and electronically provide the results to NTC-C staff. Further, according to CSI officials, NTC-C targets all shipments ATS categorizes as lower risk in an additional 6 CSI countries so that CSI targeters in those 6 countries can concentrate their reviews on the higher-risk shipments. According to CBP officials, implementation of this targeting approach allows CBP to staff high-volume ports with fewer CSI targeters. Our analysis of CSI staffing data shows that staffing of CBP targeters that support CSI at the NTC-C increased by 56 percent from fiscal years 2009 through 2012—from 27 to 42. Changes in CBP’s staffing of in-country targeters are discussed below.

Regional hub model. In 2011 and 2012, CBP implemented a regional hub model whereby CSI targeters are stationed at one port but target for multiple ports within the same country to reduce staff and thereby increase efficiencies. Under this targeting approach, host government Customs officials at remote ports complete the container examinations and electronically provide the results to CSI targeters at the regional hub. According to CBP host government officials, implementation of the regional hub is possible because of improvements in technology that allow for better and more timely transmission of image scans. Of the 13 countries with multiple CSI ports, 3 employ the regional hub model—England, France, and Italy. CBP officials reported that since implementing

⁴⁷GAO, *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).

⁴⁸NTC-C analyzes advance cargo information using ATS prior to U.S.-bound cargo being loaded on to vessels in foreign ports. NTC-C also promotes information sharing with other federal agencies and foreign governments to detect and address threats at U.S. and foreign ports.

the regional hub model, CBP has reduced the number of CSI targeters in these 3 countries by 45 percent—from 20 in October 2011 to 11 as of April 2013. According to both CBP targeters stationed in England and their British counterparts, implementation of the regional hub model has not affected the quality or number of scans of U.S.-bound container shipments.

Although implementation of the regional hub model increases efficiencies, CBP officials stated that they do not have plans to implement the regional hub model in other countries in the near future because of host country political and legal reasons. For example, CBP officials told us that CBP considered implementing the regional hub model in one country; however, the host government preferred to maintain the face-to-face interaction between the CSI targeters and their host government counterparts at each CSI port as a means to improve information exchanges and increase collaboration. Further, according to CBP and government officials in one country, a national law precludes the transmission of electronic scanned images other than to host government Customs officials. As a result, CSI targeters must be present at each CSI port in order to view the scanned container images.

In-country CSI targeters. Where possible, CBP has shifted from the initial CSI targeting approach that was heavily dependent on the placement of targeters at foreign ports to an approach that takes advantage of improvements in technologies for transmitting image scans, as addressed earlier. Specifically, from fiscal years 2009 through 2012, CBP reduced the number of CSI targeters stationed at foreign ports by 50 percent—from 153 to 77. However, as noted above, CBP increased the number of CSI targeters stationed at the NTC-C during the same time period. CBP maintains in-country targeters in 20 of the 34 CSI countries. A key benefit of maintaining CSI targeters at these ports is the relationship built with host government counterparts. CSI targeters in all 6 foreign countries we visited and host government officials in 5 of the 6 countries we visited told us that personal relationships and trust that are established between CSI targeters and host country government officials from having the CSI targeters in country are fundamental to the success of the CSI program.⁴⁹ In particular, the CSI targeters and host government

⁴⁹Officials in one foreign country we visited stated that in-country CBP targeters were not important for successful CSI operations.

officials in these 5 countries agree that the physical presence of CSI staff increases information sharing and improves collaboration. Further, host country Customs officials in 3 of the 6 countries we visited stated that the presence of CSI targeters contributed to the development or enhancement of their countries' cargo targeting programs.

According to our review of CBP performance data, changes in staffing levels in recent years have not negatively affected the effectiveness of the CSI program. In particular, CBP tracks two performance measures—(1) the percentage of U.S.-bound cargo container shipments that are reviewed by CSI targeters and (2) the percentage of U.S.-requested cargo examinations that are completed by host countries. According to CBP data from fiscal years 2009 through 2012, CSI targeters met their target goal of reviewing 100 percent of the U.S.-bound cargo shipments. Moreover, the percentage of U.S.-requested examinations of U.S.-bound cargo shipments completed by host countries increased from 93 percent in fiscal year 2009 to 98 percent in fiscal year 2012, although CBP did not meet the target goal of 100 percent. CBP reported that CSI relies on the voluntary cooperation of host nation Customs officials and that CBP works with the host ports to resolve examination issues as they arise in an effort to increase the percentage of U.S.-bound shipments that are examined.

CBP Has Made Efforts to Expand the Scope of CSI beyond WMD to Improve Effectiveness

CBP has made efforts to expand the scope of CSI targeting beyond WMD, where possible, in an effort to increase the effectiveness of the CSI program. While the priority focus of CSI is to prevent WMD and other terrorist contraband from entering the United States through cargo containers, the April 2011 CSI Statement of Policy and Intent prioritized expanding the scope of CSI beyond WMD, among other things. In particular, according to the CSI Strategy Action Plan, as well as CSI program officials with whom we met, CBP is negotiating with government officials in foreign countries where CBP has CSI targeters to expand the focus of CSI's targeting efforts beyond WMD to include other contraband, such as illicit drugs, illegal weapons, and counterfeit goods (intellectual property right violations). The CBP officials we met with noted, however, that expanding the scope of CSI targeting efforts beyond WMD is ultimately at the discretion of the host governments with whom CBP has negotiated guidelines for CSI program operations. While two of the six CSI countries that we visited allow CSI staff to target U.S.-bound cargo container shipments for contraband other than WMD, the remaining four countries generally limit targeting and examinations to cargo containers suspected of containing WMD. Government officials from one of these four countries stated it is CBP's responsibility to scan containers for other

suspected contraband, such as illicit drugs, once the containers arrive in the United States. Customs officials from another one of these four countries stated they do not have the resources to devote to scanning U.S.-bound containers that may be at risk for containing contraband other than WMD. According to CBP officials, though, expanding the scope of targeting at foreign ports by its CSI targeters has not resulted in additional costs to CBP in terms of numbers of targeters or funding.

Conclusions

Reducing risks to the global maritime supply chain is critical because foreign ports and the cargo carried by vessels from these ports are vital to the U.S. economy. DHS has made progress in reducing some maritime supply chain risks through its various maritime container security programs. The Coast Guard has developed a port security risk model that it annually updates and uses to assess port facility security, inform operational decisions, and direct resources. In contrast, CBP has not assessed the risks of foreign ports that ship cargo to the United States to determine whether its existing CSI locations remain valid since 2005. Although there have been no known incidents of cargo containers being used to transport WMD, the maritime supply chain remains vulnerable to attacks. We recognize that it may not be possible to include all of the higher-risk ports in CSI because CSI requires the cooperation of sovereign foreign governments. However, DHS and GAO risk management practices state that agencies should periodically evaluate the effectiveness of their programs and that mechanisms should be in place for altering a program based on current risk data. Periodically assessing the risk level of cargo shipped from foreign ports and using the results of these risk assessments to inform any future expansion of CSI to additional locations as well as determining whether changes need to be made to existing CSI ports would help ensure that CBP 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 maritime supply chain.

Recommendations for Executive Action

To better ensure the effectiveness of the CSI program, we recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to 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 (1) inform any future expansion of CSI to additional locations and (2) determine whether changes need to be made to existing CSI ports and make adjustments as appropriate and feasible.

Agency Comments and Our Evaluation

In August 2013, we requested comments on a draft of this report from the Departments of Homeland Security and State. Both departments provided technical comments, which we have incorporated into the report, as appropriate. In addition to its technical comments, DHS provided an official letter for inclusion in the report, which can be seen in appendix II. In its letter, DHS stated it concurred with the recommendation and plans to develop a process for conducting periodic assessments of the supply chain security risks from all ports that ship cargo to the United States and use information from the assessments to determine if future expansion or adjustments to CSI locations are 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 report date. At that time, we will send copies to the Secretaries of State and Homeland Security, appropriate congressional committees, and other interested parties. This report will also be available at no charge on GAO's website at <http://www.gao.gov>.

If you or your staff have any questions, 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 report. Staff acknowledgments are provided in appendix III.



Stephen L. Caldwell
Director
Homeland Security and Justice

Appendix I: Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection

This appendix provides information on the foreign ports that either participate directly in the Container Security Initiative (CSI) program or that U.S. Customs and Border Protection (CBP) otherwise coordinates with to review and secure U.S.-bound cargo container shipments. As of July 2013, CBP was coordinating targeting of U.S.-bound cargo container shipments with 61 foreign ports. Table 2 lists these ports according to the date the ports began conducting operations with CBP and also provides information on, among other things, the volume of U.S.-bound shipments passing through the seaport in fiscal year 2012 and the targeting approach employed.

Table 2: Foreign Ports That CBP Coordinates with Regarding Maritime Container Shipment Examinations, as of July 2013 (Listed by Date Port Began CSI Operations)

	Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach
1	Vancouver	Canada	2/20/2002	75,226	Remote ^a
2	Halifax	Canada	3/25/2002	11,731	Remote
3	Montreal	Canada	3/25/2002	257	Remote
4	Rotterdam	Netherlands	9/2/2002	177,448	In-country ^b
5	Le Havre	France	12/2/2002	130,577	Regional hub ^c
6	Bremerhaven	Germany	2/2/2003	379,662	In-country
7	Hamburg	Germany	2/9/2003	184,163	In-country
8	Antwerp	Belgium	2/23/2003	268,479	In-country
9	Singapore	Singapore	3/10/2003	428,730	NTC-C support ^d
10	Yokohama	Japan	3/24/2003	42,953	In-country
11	Hong Kong	China	5/5/2003	938,821	NTC-C support
12	Gothenburg	Sweden	5/23/2003	14,007	In-country
13	Felixstowe	United Kingdom	5/24/2003	54,926	Regional hub/NTC-C support
14	Genoa	Italy	6/16/2003	151,464	Regional hub
15	La Spezia	Italy	6/23/2003	139,382	Regional hub
16	Busan	South Korea	8/4/2003	867,627	NTC-C support
17	Durban	South Africa	12/1/2003	11,807	In-country
18	Port Kelang	Malaysia	3/8/2004	7,393	In-country
19	Tokyo	Japan	5/21/2004	139,659	NTC-C support
20	Piraeus	Greece	7/27/2004	9,746	Remote
21	Algeciras	Spain	7/30/2004	33,733	In-country
22	Kobe	Japan	8/6/2004	77,790	In-country

**Appendix I: Information on Foreign Ports That
Coordinate Maritime Cargo Container Security
Efforts with U.S. Customs and Border
Protection**

Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach
23 Nagoya	Japan	8/6/2004	74,402	In-country
24 Laem Chabang	Thailand	8/13/2004	95,551	In-country
25 Tanjung Pelepas	Malaysia	8/16/2004	84,337	In-country
26 Naples	Italy	9/30/2004	19,024	Regional hub
27 Liverpool	United Kingdom	10/19/2004	35,273	Regional hub/NTC-C support
28 Thamesport	United Kingdom	10/19/2004	27,818	Regional hub/NTC support
29 Southampton	United Kingdom	10/19/2004	50,357	Regional hub/NTC-C support
30 Tilbury	United Kingdom	10/19/2004	2,382	Regional hub/NTC-C support
31 Gioai Tauro	Italy	10/29/2004	12,381	Regional hub
32 Zeebrugge	Belgium	10/29/2004	25	In-country ^e
33 Livorno	Italy	12/16/2004	77,299	Regional hub
34 Marseilles	France	1/7/2005	16,378	Regional hub
35 Dubai	United Arab Emirates	3/26/2005	13,350	In-country
36 Shanghai	China	4/12/2005	1,900,294	NTC-C support
37 Shenzhen	China	6/24/2005	1,475,210	NTC-C support
38 Kaohsiung	Taiwan	7/25/2005	630,732	NTC-C support
39 Santos	Brazil	9/21/2005	50,816	In-country
40 Colombo	Sri Lanka	9/29/2005	127,432	In-country
41 Buenos Aires	Argentina	11/17/2005	20,791	In-country
42 Lisbon	Portugal	12/14/2005	36,903	In-country
43 Port Salalah	Oman	3/8/2006	97,450	In-country
44 Puerto Cortes	Honduras	3/25/2006	67,996	In-country
45 Auckland ^f	New Zealand	4/1/2006	47,244	Remote
46 Chi-lung	Taiwan	9/25/2006	97,476	In-country
47 Valencia	Spain	9/25/2006	106,118	In-country
48 Caucedo	Dominican Republic	9/26/2006	24,843	In-country
49 Barcelona	Spain	9/27/2006	41,763	In-country
50 Kingston	Jamaica	9/28/2006	75,607	In-country
51 Freeport	Bahamas	9/29/2006	66,912	In-country
52 Qasim	Pakistan	4/30/2007	46,486	Remote
53 Shekou	China ^f	08/01/2007	60,019	NTC-C support
54 Chiwan	China	8/1/2007	138,069	NTC-C support
55 Balboa	Panama	8/27/2007	76,380	In-country

Appendix I: Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection

Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach	
56	Cartagena	Colombia	9/13/2007	52,682	In-country
57	Ashdod	Israel	9/17/2007	543	Remote
58	Haifa	Israel	9/25/2007	36,490	Remote
59	Colon	Panama	9/28/2007	50,481	In-country
60	Manzanillo	Panama	9/28/2007	77,030	In-country
61	Melbourne ^f	Australia	11/1/2011	37,730	Remote

Source: GAO presentation of CBP data.

^aThe remote targeting approach relies on host government Customs officials to complete the container examinations and electronically provide the results of any container image scans to U.S.-based CBP targeters.

^bThe in-country targeting approach places CBP targeters at CSI ports, who directly coordinate with host government Customs officials to examine containers and obtain the results of the examinations.

^cUnder the regional hub targeting approach, CSI staff are stationed at one port but target for multiple ports within the same country to increase efficiencies. Host government Customs officials at remote ports complete the container examinations and electronically provide the results to CSI targeters at the regional hub.

^dThe National Targeting Center-Cargo (NTC-C) targeting approach relies on in-country CBP targeters to review higher-risk shipments and U.S.-based CBP targeters to review lower-risk shipments. NTC-C analyzes advance cargo information before shipments reach the United States.

^eAccording to CBP officials, CSI targeters in Antwerp also target U.S.-bound container shipments exported from Zeebrugge and drive to that port to participate in examinations, as necessary.

^fAccording to CBP officials, CBP entered into arrangements with New Zealand and Australia to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

September 4, 2013

Stephen L. Caldwell
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-13-764, "SUPPLY CHAIN SECURITY: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of the progress DHS has made in reducing some maritime supply chain risks through its various maritime container security programs, including efforts by the U.S. Coast Guard and U.S. Customs and Border Protection (CBP). DHS also appreciates GAO's recognition that it may not be possible to include all of the higher-risk ports in the Container Security Initiative (CSI) because CSI requires the cooperation of sovereign foreign governments. DHS, however, is committed to deploying CBP officers as part of multi-disciplinary CSI teams to work with host nation counterparts to target high-risk cargo containers and protect containerized shipping from exploitation by terrorists.

The draft report contained one recommendation with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to:

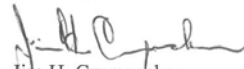
Recommendation: Periodically assess the supply chain security risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to (1) inform any future expansion of CSI to additional locations and (2) determine whether changes need to be made to existing CSI ports and make adjustments as appropriate and feasible.

Response: Concur. With input from relative stakeholders, CBP's Office of Field Operations will formulate a process for conducting periodic assessments of the supply chain security risks from all ports that ship cargo to the U.S. CBP anticipates that its first assessment will be completed by August 12, 2014. The information from that assessment will then be used to determine what, if any, future expansion and/or adjustments to the CSI locations are appropriate. Estimated Completion Date: December 31, 2014.

**Appendix II: Comments from the Department
of Homeland Security**

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker
Director

Departmental GAO-OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Christopher Conrad (Assistant Director), Josh Diosomito, and Paul Hobart made key contributions to this report. Also contributing to this report were Charles Bausell, Frances Cook, Stanley Kostyla, and Lara Miklozek.

Related GAO Products

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

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

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

Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning. [GAO-12-422T](#). Washington, D.C.: February 7, 2012.

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.

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.

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.

Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security. [GAO-05-404](#). Washington, D.C.: March 11, 2005.

Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors. [GAO-03-770](#). Washington, D.C.: July 25, 2003.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

