

August 2008

SUPPLY CHAIN SECURITY

CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain





Highlights of [GAO-08-538](#), a report to congressional requesters

Why GAO Did This Study

Oceangoing cargo containers play a vital role in global trade but can also pose a risk of terrorist exploitation. U.S. Customs and Border Protection (CBP), part of the Department of Homeland Security (DHS), oversees security of the supply chain—the flow of goods from manufacturer to retailer. CBP anticipates that adoption of uniform, international customs security standards could eventually lead to a system of mutual recognition whereby the customs security-related practices and programs taken by one customs administration are recognized and accepted by another administration. In response to congressional requesters, GAO determined (1) actions CBP has taken to develop and implement international supply chain security standards, (2) actions CBP has taken with international partners to achieve mutual recognition of customs security practices, and (3) issues CBP and foreign customs administrations anticipate in implementing 100 percent scanning of U.S.-bound container cargo. To conduct its work, GAO analyzed CBP documents on supply chain security programs and international cooperation initiatives and met with CBP officials and foreign customs officials from various trading partner nations. Also, GAO drew upon its related reports and testimony on supply chain security issued earlier this year—[GAO-08-187](#) (Jan. 25), [GAO-08-240](#) (Apr. 25), and [GAO-08-533T](#) (June 12). DHS provided technical comments on a draft of this report, which GAO incorporated where appropriate.

To view the full product, including the scope and methodology, click on [GAO-08-538](#). For more information, contact Stephen Caldwell at (202) 512-9610 or Caldwells@gao.gov.

SUPPLY CHAIN SECURITY

CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain

What GAO Found

To develop and implement international supply chain security standards, CBP has taken a lead role in working with foreign customs administrations and the World Customs Organization (WCO). Through the Container Security Initiative (CSI), CBP places staff at foreign seaports to work with host nation customs officials to identify high-risk container cargo bound for the United States, and through the Customs-Trade Partnership Against Terrorism (C-TPAT), CBP forms voluntary partnerships to enhance security measures with international businesses involved in oceangoing trade with the United States. In collaboration with 11 other members of the WCO, CBP developed the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), which is based in part on the core concepts of the CSI and C-TPAT programs and provides standards for collaboration among customs administrations and entities participating in the supply chain. The SAFE Framework was adopted by the 173 WCO member customs administrations in June 2005; and as of July 2008 154 had signed letters of intent to implement the standards.

CBP has actively engaged with international partners to define and achieve mutual recognition of customs security practices. Broadly, for example, CBP contributed to development of the SAFE Framework, which calls for a system of mutual recognition. More specifically, in June 2007, CBP signed a mutual recognition arrangement with New Zealand—the first such arrangement in the world—to recognize each other's customs-to-business partnership programs. Furthermore, in June of this year, CBP signed mutual recognition agreements with Jordan and Canada. By early 2009, CBP anticipates obtaining a mutual recognition agreement with the European Commission, which represents the 27 member nations of the European Union.

CBP actively engages in the implementation of international customs security standards, however recent law, such as The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) requiring that 100 percent of U.S.-bound container cargo be scanned at foreign seaports—using a nonintrusive inspection process involving equipment such as X-rays and radiation detection equipment—may affect worldwide adoption of international supply chain security standards. CBP and some foreign partners have stated that unless additional resources are made available, 100 percent scanning could not be met. Given limited resources, CBP and European custom administration officials said that 100 percent scanning may provide a lower level of security if customs officers are diverted from focusing on high-risk container cargo. Under the current risk-management system, for example, the scanned images of high-risk containers are to be reviewed in a very detailed manner. However, according to WCO and industry officials, if all containers are to be scanned, the reviews may not be as thorough. Further, a European customs administration reported that 100 percent scanning could have a negative impact on the flow of commerce and also would affect trade with developing countries disproportionately.

Contents

Letter		1
	Results in Brief	5
	Background	7
	CBP and Foreign Customs Administrations Have Jointly Developed Global Customs Security Standards and Initiatives and Work Cooperatively to Implement These Standards Worldwide	14
	CBP Is Working with Foreign Customs Administrations to Develop International Standards for Customs-to-Customs Relationships and for Customs-to-Business Partnership Programs	14
	CBP and International Partners Are Working to Achieve Mutual Recognition of Customs Security Practices	23
	While Working to Internationalize Customs Security Standards, CBP and International Partners Report Challenges in Balancing These Efforts with Other Legal Requirements	31
	Concluding Observations	34
	Agency Comments	35
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	World Customs Organization SAFE Framework of Standards	41
Appendix III	CBP's Collaborative Efforts to Enhance Container Security	44
Appendix IV	The Secure Freight Initiative	47
Appendix V	GAO Contact and Staff Acknowledgments	50
Related GAO Products		51

Tables

Table 1: Major U.S. Initiatives to Secure Oceangoing Containers	9
Table 2: U.S.-EU Joint Customs Cooperation Committee Action Plan as of June 2008	29
Table 3: WCO SAFE Framework—Standards for the Customs-to-Customs Pillar	42
Table 4: WCO SAFE Framework—Standards for the Customs-to-Business Pillar	43
Table 5: CBP’s Collaborative Efforts to Enhance Container Security	44
Table 6: Information on the Six Foreign Seaports Participating in the SFI Pilot Program	48

Figures

Figure 1: Overview of Key Participants Involved in Shipping Containers in the International Supply Chain	8
Figure 2: CSI Targeting and Examination Activities	11
Figure 3: Timeline of Major U.S. and International Events to Facilitate Supply Chain Security	13
Figure 4: World Map Indicating the 154 WCO Member Countries That Have Signed Letters of Intent to Implement the WCO SAFE Framework	16
Figure 5: The Twin Pillars of Customs-to-Customs Network Arrangements and Customs-to-Business Partnership Programs Based on the Four Core Principles of the WCO SAFE Framework of Standards	18
Figure 6: Two Forms of Mutual Recognition	25

Abbreviations

9/11 Act	Implementing Recommendations of the 9/11 Commission Act
AEO	Authorized Economic Operator
APEC	Asia-Pacific Economic Cooperation
ATS	Automated Targeting System
C-TPAT	Customs-Trade Partnership Against Terrorism
CBP	Customs and Border Protection
CSI	Container Security Initiative
DHS	Department of Homeland Security
DOE	Department of Energy
EU	European Union
JCCC	Joint Customs Cooperation Committee
NTC-C	National Targeting Center--Cargo
SAFE Port Act	Security and Accountability for Every Port Act
SAFE Framework	WCO Framework of Standards to Secure and Facilitate Global Trade
SFI	Secure Freight Initiative
WCO	World Customs Organization
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. It 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.



United States Government Accountability Office
Washington, DC 20548

August 15, 2008

Congressional Requesters

Concerns about the ability of both the federal government and U.S. companies participating in international maritime commerce to identify and prevent weapons of mass destruction (WMD) from being smuggled inside cargo containers bound for the United States have heightened since the terrorist attacks of 2001. Oceangoing cargo containers play a vital role in the movement of cargo between global trading partners, and more than 700 foreign seaports ship cargo to the United States. In fact, 11 million oceangoing cargo containers arrived at U.S. seaports in fiscal year 2007—meaning roughly 30,000 oceangoing containers arrived each day that year. Balancing security concerns with the need to facilitate the free flow of commerce remains an ongoing challenge for the public and private sectors alike.

In the federal government, U.S. Customs and Border Protection (CBP), part of the Department of Homeland Security (DHS), is responsible for overseeing oceangoing container security and reducing the vulnerabilities associated with the supply chain—the flow of goods from manufacturers to retailers. As CBP performs this mission, it maintains two overarching and sometimes conflicting goals—increasing security while facilitating legitimate trade and travel. To address these goals, CBP has developed a layered risk-management approach to cargo security.¹ This approach includes analyzing trade data received in advance of cargo being shipped to facilitate risk-based decisions for the identification of high-risk cargo. Also, as part of this risk-management approach, CBP operates two voluntary security programs. The first is the Container Security Initiative (CSI), a customs-to-customs program that places CBP officers in foreign seaports to use intelligence and risk assessment information to determine whether U.S.-bound shipments are at risk of containing WMD or other

¹Risk 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. Risk management allows for reduction of risk against possible terrorist attack to the nation by allocating resources to those areas of highest risk and is an approach that has been accepted throughout the federal government.

terrorist contraband—a process referred to as targeting.² The second is the Customs-Trade Partnership Against Terrorism (C-TPAT), a customs-to-business partnership program that provides benefits to supply chain companies that comply with pre-determined security measures.³ In addition, to better protect international trade against the threat of terrorism, CBP promotes a set of international customs security standards similar to the CSI and C-TPAT programs, which as of June 2008, 154 countries have pledged to adopt. To develop and promote the implementation of these international standards for supply chain security, CBP works through the World Customs Organization (WCO)—an intergovernmental organization representing the customs administrations of 173 countries, which aims to enhance the effectiveness and efficiency of customs administrations. CBP and the WCO anticipate that widespread adoption of uniform, international customs security standards eventually could lead to the development of a system of mutual recognition whereby the security-related practices and programs taken by the customs administration of one country are recognized and accepted by the administration of another. According to CBP, a system of mutual recognition could lead to greater efficiency in providing security by, for example, reducing redundant examinations of container cargo and avoiding the unnecessary burden of addressing different sets of requirements as a shipment moves through the supply chain in different countries, thereby facilitating international trade.

To further address container security concerns, Congress passed, and the President signed, the Security and Accountability for Every (SAFE) Port Act in 2006, which includes provisions that codified the CSI and C-TPAT programs, both of which had been CBP initiatives but not previously required by law.⁴ The act also included requirements for CBP to consider factors such as cargo volume when designating seaports as CSI participants and required CBP to test the feasibility of scanning 100 percent of U.S.-bound container cargo in foreign seaports. To fulfill these

²For more information on the CSI program, see GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, [GAO-08-187](#) (Washington, D.C.: Jan. 25, 2008).

³For more information on the C-TPAT program, see GAO, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, [GAO-08-240](#) (Washington, D.C.: Apr. 25, 2008).

⁴Pub. L. No. 109-347, 120 Stat. 1884.

and other requirements of the act, CBP developed the Secure Freight Initiative (SFI) and the SFI pilot program.⁵ In August 2007, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) was enacted, requiring, among other things, that foreign seaports scan 100 percent of U.S.-bound container cargo by 2012, with possible exemptions for individual seaports,⁶ replacing the similar provision in the SAFE Port Act that did not have a deadline for full implementation of the scanning requirement.⁷

In response to your request, we assessed CBP's efforts related to international customs security standards. Specifically, this report addresses the following questions:

- What actions has CBP taken to develop and implement international supply chain security standards?
- What actions has CBP taken with international partners to achieve mutual recognition of customs security practices?
- What issues do CBP and foreign customs administrations working to internationalize customs security standards anticipate in implementing 100 percent scanning of U.S.-bound container cargo?

To address these objectives, we reviewed available CBP documentation, such as reports pertaining to the CSI, C-TPAT, and SFI programs, and international agreements related to CBP's work in the international trade community. In addition, we met with CBP officials in Washington, D.C., who have program responsibilities for international affairs and trade. Also, to discuss multilateral and bilateral efforts to promote supply chain security, we met with representatives from the European Commission and the WCO, as well as with customs officials from the Americas, Asia, and Europe at the 2007 WCO World Customs Forum and CBP's 2007 CSI

⁵The SFI pilot program tests the feasibility of 100 percent scanning at a select number of foreign seaports involved in the CSI program. See appendix V for more information on SFI and its pilot program.

⁶The 9/11 Act includes possible exceptions for seaports for which DHS certifies that specified conditions exist. Among others, these conditions are: (1) adequate scanning equipment is not available or cannot be integrated with existing systems, (2) a port does not have the physical characteristics to install the equipment, or (3) use of the equipment will significantly impact trade capacity and the flow of cargo.

⁷Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

Global Targeters Conference.⁸ We also spoke with representatives of industry groups, including CBP's Departmental Advisory Committee on Commercial Operations and the Federation of European Private Port Operators.⁹ We spoke with officials of foreign customs administrations during our visits to 6 of the 58 seaports that participate in the CSI program.¹⁰ We selected the six CSI seaports—located in the countries of Belgium, Canada, France, Honduras, South Korea, and United Arab Emirates—based on geographic and strategic significance, container volume shipped to the United States from the seaports, and when the seaports began conducting CSI operations. The results from our visits to seaports provided examples of CBP and host government operations but cannot be generalized beyond the seaports visited because we did not use statistical sampling techniques in selecting the seaports. Similarly, while the perspectives of foreign officials we spoke to cannot be generalized across the wider population of countries, they provided us examples of how CBP interacts with foreign customs administration officials at overseas seaports. Additionally, we reviewed CBP and WCO documents on international initiatives for enhancing supply chain security. We conducted this performance audit in conjunction with concurrent reviews of the CSI and C-TPAT programs from May 2006 through July 2008 in accordance with generally accepted government auditing standards.¹¹ Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained

⁸The European Commission is the European Union's (EU) policy making and executive engine. The commission is composed of 27 commissioners, one from each member state. Among its many powers, the commission proposes legislation for approval by the EU Council and European Parliament in matters relating to economic integration, ensures that EU laws are applied and upheld throughout the EU, implements the budget, and represents the European Community in international trade negotiations. The EU is composed of 27 independent sovereign countries which are known as member states: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

⁹CBP's Departmental Advisory Committee on Commercial Operations was originally established by the Omnibus Budget Reconciliation Act of 1987, and its purpose is to advise the Secretaries of the Department of the Treasury and the DHS on the commercial operations of CBP and related DHS and Treasury functions. The Federation of European Private Port Operators is a private industry organization representing the interests of about 800 private port operators in Europe.

¹⁰The 58 CSI seaports are located in 33 different countries.

¹¹See [GAO-08-187](#) and [GAO-08-240](#).

provides a reasonable basis for our findings and conclusions based on our audit objectives. A detailed discussion of our scope and methodology is contained in appendix I.

Results in Brief

CBP has taken a lead role in working with members of the international customs community—including foreign customs administrations in the WCO and relevant private industry groups—to develop and implement international supply chain security standards. CBP, along with 11 other members of the WCO, developed the Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework) that was adopted in June 2005 by the 173 member customs administrations of the WCO. The SAFE Framework—which is based on CBP’s CSI and C-TPAT programs—provides guidance to WCO member customs administrations on (1) customs-to-customs practices that assist in securing the international supply chain against terrorism and other forms of transnational crimes and (2) the development of customs-to-business partnership programs such as the C-TPAT program. Working with international partners, CBP has assisted in the international implementation of the SAFE Framework by participating in a capacity-building program that provides technical assistance and training to the customs administrations of developing countries. In addition to working through the WCO to promote international customs security standards, CBP’s CSI and C-TPAT programs have influenced the development of similar programs in other countries because their programs provide models for how to implement the security standards in the SAFE Framework.

CBP has worked with the international customs community to achieve a system of mutual recognition—an arrangement whereby the actions or decisions taken by one customs administration are recognized and accepted by another administration—by, among other things, adopting and implementing the SAFE Framework that calls for a system of mutual recognition, and by developing an action plan for the achievement of mutual recognition of customs-to-business partnership programs. The WCO’s SAFE Framework calls for the establishment of two types of mutual recognition—mutual recognition of customs controls and mutual recognition of customs-to-business partnership programs. According to CBP, although not easily or quickly attained, achieving mutual recognition offers the potential benefit of providing CBP an exit strategy for the CSI program in some countries. Generally, while accepting the WCO definition of mutual recognition, CBP focuses its efforts by offering guidance on and a process for achieving mutual recognition of customs-to-business

partnership programs—referred to as Authorized Economic Operator (AEO) programs. According to officials from CBP and foreign customs administrations, a system of mutual recognition will be a catalyst for further implementation of AEO programs. To work toward a system of mutual recognition of customs-to-business partnership programs, CBP engages in activities with other countries. For example, in June 2007, CBP signed a mutual recognition arrangement with New Zealand—the first such arrangement in the world—to recognize each other’s customs-to-business partnership programs and later signed mutual recognition agreements with Jordan and Canada in June 2008. Further, CBP and the European Commission have agreed to establish mutual recognition of customs-to-business partnership programs by early 2009.

CBP actively engages in the development and implementation of international customs security standards; however it may face issues in worldwide adoption of these standards because of the statutory requirement to scan 100 percent of U.S.-bound container cargo. While the pilot program is still underway and its full impacts are still unknown, international partners have expressed to DHS and Congress that 100 percent scanning runs counter to—and could adversely impact the implementation of—international customs security standards such as the SAFE Framework. Officials from the European Commission and CBP stated that unless additional resources are made available, 100 percent scanning could not be met. And as we testified in June 2008, it is unclear who will pay for additional resources—including increased staff, equipment, and infrastructure—needed to implement the statutory requirement to scan 100 percent of U.S.-bound container cargo at foreign seaports. Given these resource issues, officials from CBP and European customs administrations stated that scanning all cargo bound for the United States may actually provide a lower level of security. The officials explained that 100 percent scanning could result in diluting the current focus on high-risk containers. Under the current risk-management system, customs officers are to base their reviews on the perceived risk posed by the cargo and, thus, are to review the scanned images of high-risk containers in a very thorough and detailed manner. However, according to CBP and WCO officials, if the scanned images of all containers must be reviewed, the reviews may not be as thorough because customs officers could lose focus due to the sheer volume of work. If images are not properly or thoroughly analyzed, a degradation of security could result. Further, a European customs administration official reported that 100 percent scanning could have a negative impact on the flow of international commerce. The official also added that the 100 percent scanning

requirement would disproportionately affect trade with developing countries.

In commenting on a draft copy of this report, DHS provided technical clarifications, which we incorporated where appropriate.

Background

Vulnerabilities of Containers in the International Supply Chain

Seaports are critical gateways for the movement of commerce through the international supply chain. The facilities, vessels, and infrastructure within seaports, and the cargo passing through them, all have vulnerabilities that terrorists could exploit. The containers carrying goods that are shipped in oceangoing vessels are of particular concern because they can be filled overseas at many different locations and are transported through complex logistics networks before reaching U.S. seaports.

In addition, transporting a shipping container from its international point of origin to its final destination involves many different participants and many points of transfer. The material in a container can be affected not only by the manufacturer or supplier of the material being shipped but also by carriers who are responsible for getting the material to a seaport and by personnel who load containers onto the ships. Others who interact with the cargo or have access to the records of the goods being shipped include exporters who make arrangements for shipping and loading, freight consolidators who package disparate cargo into containers, and forwarders who manage and process the information about what is being loaded onto the ship. Figure 1 illustrates many of the key participants and points of transfer involved from the time that a container is loaded for shipping to its arrival at the destination seaport and ultimately the importer.

Figure 1: Overview of Key Participants Involved in Shipping Containers in the International Supply Chain



Source: GAO, DHS.

Several studies of maritime security conducted by federal, academic, nonprofit, and business organizations have concluded that the movement of oceangoing cargo in containers is vulnerable to some form of terrorist action. Every time responsibility for cargo in containers changes hands along the supply chain there is the potential for a security breach; thus, vulnerabilities exist that terrorists could take advantage of by, for example, placing a WMD into a container for shipment to the United States or elsewhere. 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. Finally, while CBP has noted that the likelihood of terrorists smuggling WMDs into the United States in cargo containers is low, the nation's vulnerability to this activity and the consequences of such an attack are potentially high. For example, in 2002, Booz Allen Hamilton sponsored a simulated scenario in which the detonation of weapons smuggled in cargo containers shut down all U.S. seaports for 12 days. The results of the simulation estimated that the seaport closures could result in a loss of \$58 billion in revenue to the U.S. economy along with significant disruptions to the movement of trade.

The U.S. Government Is Engaged in Efforts to Secure Containers in the International Supply Chain

The federal government has taken many steps to secure the supply chain, including the cargo in oceangoing containers destined for the United States. While CBP officials at domestic seaports continue efforts to identify and examine high-risk imports arriving in containers, CBP's post-9/11 strategy also involves focusing security efforts beyond U.S. borders to target and examine high-risk cargo before it enters U.S. seaports. As discussed earlier in this report, CBP's strategy is based on a layered approach of related initiatives that attempt to focus resources on potentially risky cargo shipped in containers while allowing other containers carrying cargo to proceed without unduly disrupting commerce into the United States. While the Department of Energy (DOE) has led U.S. efforts to detect radiation in cargo containers originating at foreign seaports, CBP has initiated five initiatives addressing container security. A brief description of each is shown in table 1.

Table 1: Major U.S. Initiatives to Secure Oceangoing Containers

Initiative and year introduced	Department	Description
Automated Targeting System (ATS), 1999	DHS	ATS is a complex mathematical model that uses weighted rules to assign a risk score to arriving cargo shipments based on shipping information. ATS helps CBP identify and prevent potential terrorists and terrorist weapons from entering the United States. CBP uses this computerized decision support tool to review documentation, including electronic cargo manifest ^a information submitted by the ocean carriers on all arriving shipments, and entry data (more detailed information about the cargo) submitted by brokers to develop risk scores that help identify containers for additional examination.
24-hour Rule, 2002	DHS	CBP generally requires ocean carriers to electronically transmit cargo manifests and entry data to CBP's Automated Manifest System—a system designed to control imported merchandise from the time a carrier's cargo manifest is submitted to CBP until the cargo is properly entered and released by CBP—24 hours before the U.S.-bound cargo is loaded onto a vessel at a foreign seaport. Carriers and importers are to provide information to CBP that is used by ATS in deriving risk scores. The cargo manifest information is submitted by ocean carriers on all arriving cargo shipments, and entry data are submitted by brokers.
Container Security Initiative (CSI), 2002	DHS	CBP, through the CSI program, places staff at participating foreign seaports to work with host country customs officials to identify and examine high-risk cargo to be shipped in containers for WMD before they are shipped to the United States. CBP officials identify the high-risk containers and request that their foreign counterparts examine the contents of the containers.
Customs-Trade Partnership Against Terrorism (C-TPAT), 2001	DHS	CBP develops voluntary partnerships with members of the international trade community comprised of importers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies agree to improve the security of their supply chains in return for various benefits, such as a reduced likelihood that their containers will be examined. As of May 2008, there were over 8,400 C-TPAT members from the international trade community that had various roles in the supply chain.



Initiative and year introduced	Department	Description
Megaports Initiative, 2003	DOE	DOE installs radiation detection equipment at key foreign seaports, enabling foreign government personnel to use radiation detection equipment to screen shipping containers entering and leaving these seaports, regardless of the containers' destination, for nuclear and other radioactive material that could be used against the United States and its allies.
Secure Freight Initiative, 2007	DHS, DOE	Pilot program at six selected CSI seaports to scan 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas using integrated examination systems that couple nonintrusive inspection equipment and radiation detection equipment.

Source: GAO summary of information obtained from DHS and DOE.

^aCargo manifests are prepared by the ocean carrier and are composed of bills of lading for each shipment of cargo loaded on a vessel to describe the contents of the shipments. The bill of lading can include a variety of other information, such as the manufacturer of the cargo and the name of the shipping line.

One of CBP's major efforts to address container security is CSI—a 6-year-old program that aims to identify and examine U.S.-bound cargo that is considered to pose a high risk of concealing WMDs or other terrorist contraband by reviewing advanced cargo information sent by ocean cargo carriers. As part of the program, CBP officers, usually stationed at foreign seaports throughout Europe, Asia, the Middle East, the Americas, or elsewhere, seek to identify high-risk U.S.-bound container cargo. CBP and host government officials share the role of assessing the risk of U.S.-bound container cargo leaving the seaports of the countries participating in CSI. Among other tasks, CBP officers at the 58 CSI seaports are responsible for identifying high-risk cargo shipped in containers, whereas host government customs officials examine the high-risk cargo—when requested by CBP—by scanning containers that hold the cargo using various types of nonintrusive inspection equipment, such as large-scale X-ray machines, or by physically searching the containers' contents before departure to the United States. Figure 2 describes the activities carried out by CBP officers and host government customs officials to target and examine high-risk container cargo at CSI seaports.

Figure 2: CSI Targeting and Examination Activities

<p>Targeting high-risk container shipments.</p> <p>CBP uses ATS to electronically review data about U.S.-bound shipments to produce a risk score, a process CBP refers to as screening. CBP officers review the ATS risk scores and may consider additional information or collaborate with host government officials to identify high-risk shipments with a nexus to terrorism—a process referred to as targeting. CBP officials make a final determination about which containers are high risk and will be referred to host government customs officials for examination.</p>	<p>CBP official conducting targeting activities.</p> 
<p>Examining high-risk container shipments.</p> <p>CBP officials request that host government officials examine containers with high-risk shipments to detect WMD or other items with a nexus to terrorism. Examining a container involves using nonintrusive inspection equipment, radiation detection equipment, or both to scan the container's contents. Typically, the radiation detection equipment is used, then large scale nonintrusive inspection equipment, to scan the container's contents. The results of the scan will influence whether or not CBP requests that the host government conduct a physical search, during which a container is opened and its contents are removed for review.</p>	<p>Container scanned with non-intrusive imaging x-ray equipment at a CSI port.</p> 

Source: GAO and CBP.

Another of CBP's major efforts to address container security is through the C-TPAT program. Initiated in November 2001, C-TPAT aims to secure the flow of goods bound for the United States by developing a voluntary antiterrorism partnership with stakeholders of the international trade community, which is comprised of importers; customs brokers; forwarders; air, sea, and land carriers; and contract logistic providers. C-TPAT members commit to improving the security of the supply chain, which may include, for example, the use of employee identification

systems for access control purposes. The members also agree to provide CBP with information on their specific security measures and allow CBP to validate or verify, among other things, that their security measures meet or exceed the agency's minimum security requirements. The purpose of this latter step, referred to as validation, is to help CBP ensure that the security measures outlined in a member's security profile are actually in place and are effective. In return, C-TPAT members are entitled to various benefits—chief among them, a reduced likelihood of having their cargo inspected.

As part of its mission and strategic plan, CBP also seeks to promote the security of oceangoing containers by having its officers work closely with other stakeholders, including international customs trade organizations and host governments (where seaports participating in the CSI program are located). CBP's former Commissioner has stated that a key goal of this outreach effort is to promote an international framework of customs security standards that multiple countries can agree upon. Such a framework is intended by the United States and other parties to help institute consistent, reliable customs security standards and practices. Figure 3 shows a timeline for the various U.S. security initiatives addressing container cargo security.

Figure 3: Timeline of Major U.S. and International Events to Facilitate Supply Chain Security

United States		International
	1999	
	Jun	<i>Revised Kyoto Convention ^a</i>
	2001	
<i>9/11 Terrorist attack</i>	Sep	
<i>C-TPAT (U.S. AEO program) established</i>	Nov	
	2002	
<i>CSI program began</i>	Jan	
	2005	
	Jun	<i>WCO adopted the SAFE Framework of Standards</i>
	2006	
	Jan	<i>WCO began capacity building programs</i>
	Mar	<i>Japan's AEO program becomes operational</i>
<i>SAFE Port Act passed</i>	Oct	
	2007	
	May	<i>Singapore's AEO program becomes operational</i>
<i>9/11 Act required 100% scanning by 2012</i>	Jun	<i>United States and New Zealand establish Mutual Recognition of their AEO programs</i>
	Aug	
<i>Initiation of Secure Freight Initiative pilot program</i>	Oct	
	2008	
	Jan	<i>EU's AEO program becomes operational</i>
<i>CBP releases report on SFI pilot program</i>	Jun	
	2009	
	Jan (projected)	<i>Mutual recognition between United States and EU AEO programs</i>

Source: GAO analysis.

^aThe Revised Kyoto Convention is an international customs agreement signed by 55 countries, including the United States. Signatories pledge to use risk management to identify high-risk container cargo.

CBP and Foreign Customs Administrations Have Jointly Developed Global Customs Security Standards and Initiatives and Work Cooperatively to Implement These Standards Worldwide

Working through the WCO and in cooperation with the international customs community, CBP has taken a lead role in the development of international standards in customs security practices and in customs-to-business partnership programs. This effort led to the adoption of the WCO SAFE Framework, which establishes standards for collaboration between the customs administrations of different countries as well as between customs administrations and businesses. CBP has also assisted in the implementation of the SAFE Framework to promote international customs security standards, such as through capacity-building efforts that provide technical assistance and training to developing countries wanting to implement the SAFE Framework.

CBP Is Working with Foreign Customs Administrations to Develop International Standards for Customs-to-Customs Relationships and for Customs-to-Business Partnership Programs

CBP has taken a lead role in working with foreign customs administrations on approaches to standardizing supply chain security worldwide. In 2004, CBP, along with 11 other member customs administrations of the WCO, formed the High Level Strategic Group to develop international standards for customs security practices.¹² The group developed the WCO Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework), the core concepts of which are based on components in CBP's CSI and C-TPAT programs. Further, CBP's CSI and C-TPAT programs have provided a model for developing global customs security standards, as countries adopt a framework that embodies the core principles of these programs.

The CSI and C-TPAT strategic plans call for promoting an international framework of customs security standards using the core elements of the U.S. cargo security strategy.¹³ As CBP has recognized in security matters the United States is not self-contained, either in its problems or its solutions. The growing interdependence of countries requires policy

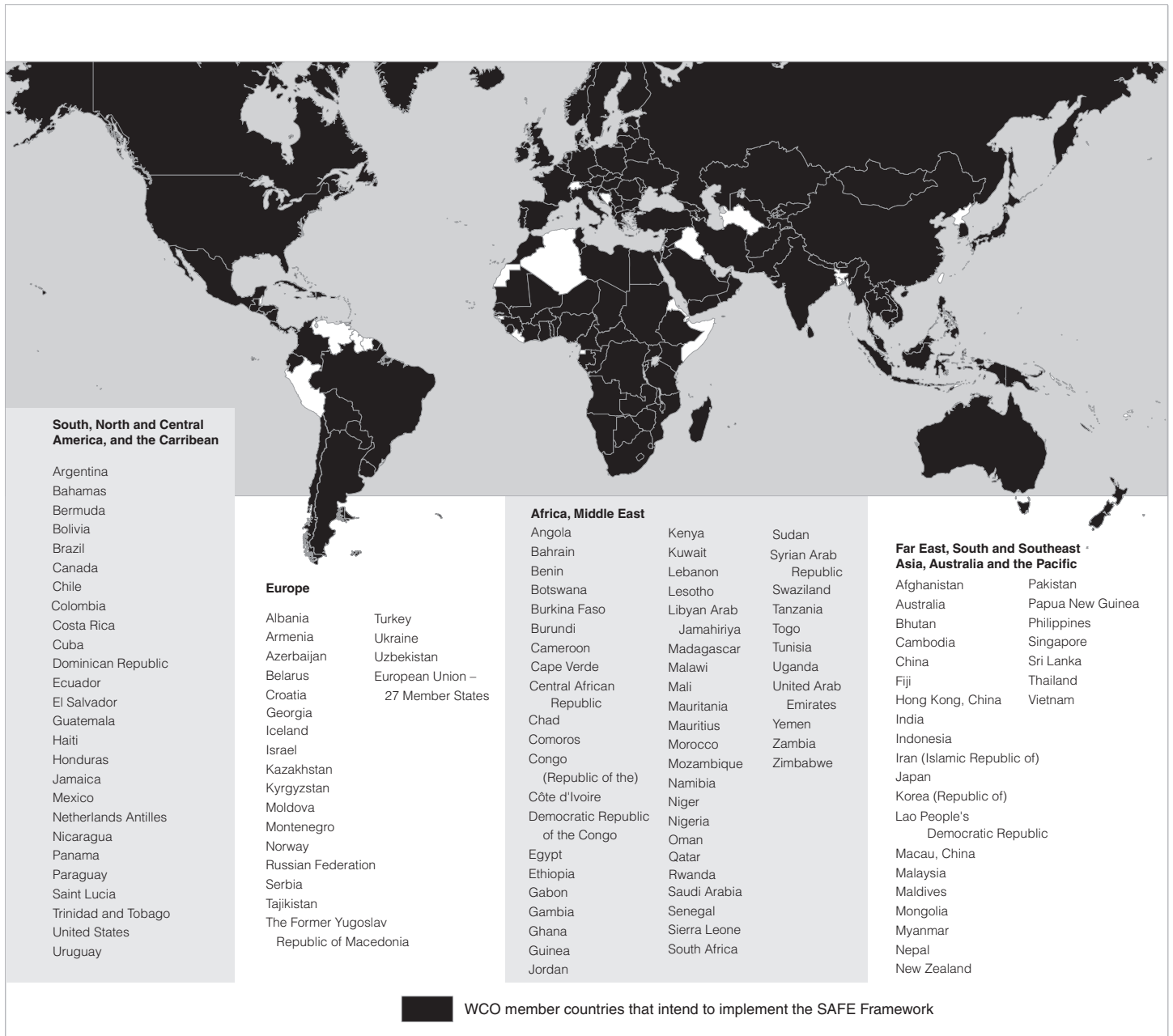
¹²The members of the High Level Strategic Group are the United States, Canada, Finland, Germany, Ghana, Hungary, India, Japan, Jordan, Senegal, South Africa, and the European Commission.

¹³The core elements of CBP's cargo security strategy include risk-based targeting, advance information requirements (such as the 24-Hour Rule), CSI, and C-TPAT. See table 1 for more details.

makers to recognize the need to work in partnerships across international boundaries to achieve vital national goals. Further, the WCO has acknowledged that customs security enforcement, particularly with the threat of terrorism, cannot be done in isolation and requires international cooperation. To that end, CBP has taken a lead role in working with foreign customs administrations, through the WCO, to establish the framework of international standards designed to enhance the security of the global supply chain while facilitating international trade. In June 2005, the 173 member customs administrations of the WCO adopted the SAFE Framework. Further, as of June 2008, 154 WCO member countries, including the United States, had signed letters of intent for implementing the SAFE Framework¹⁴ (see fig. 4).

¹⁴The WCO updated the SAFE Framework in June 2007.

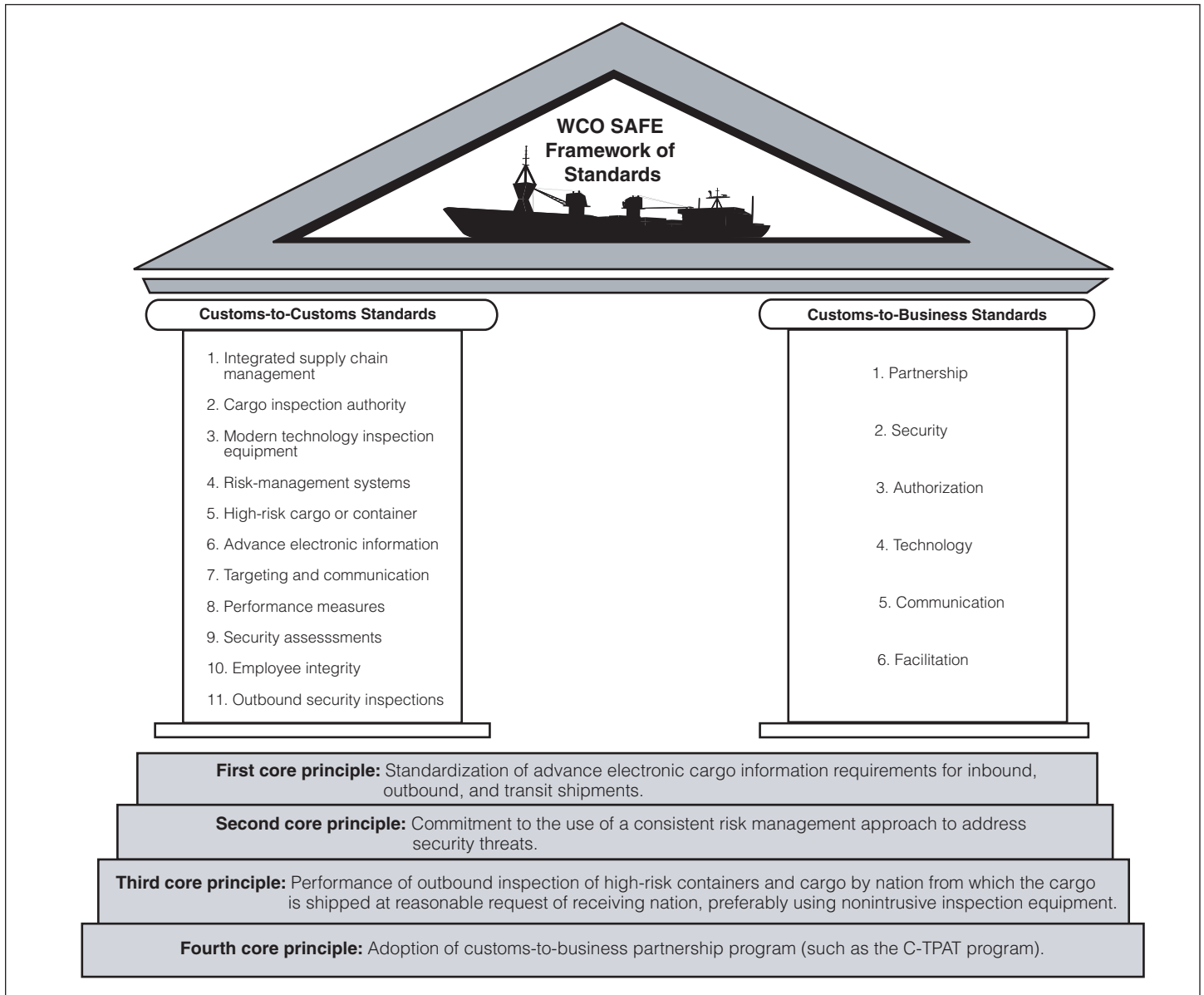
Figure 4: World Map Indicating the 154 WCO Member Countries That Have Signed Letters of Intent to Implement the WCO SAFE Framework



Source: GAO (map art), Map Resources (map), WCO (data).

The SAFE Framework establishes the standards for collaboration between the customs administrations of different countries (known as the customs-to-customs pillar) as well as between customs administrations and the businesses participating in commercial trade activities through various supply chains (known as the customs-to-business pillar). These standards provide guidance on what WCO member customs administrations must do at a minimum to both secure the international supply chain and facilitate trade. As seen in figure 5, the twin pillars of the customs-to-customs standards and the customs-to-business standards are based upon four core principles and underpin the SAFE Framework.

Figure 5: The Twin Pillars of Customs-to-Customs Network Arrangements and Customs-to-Business Partnership Programs Based on the Four Core Principles of the WCO SAFE Framework of Standards



Source: GAO representation of WCO data and Art Explosion images.

Note: Appendix II describes the 11 standards of the customs-to-customs pillar and the 6 standards of the customs-to-business pillar.

The standards and principles of the SAFE Framework are similar to those of the CSI and C-TPAT programs. For example, just as in the CSI program, the standards in the customs-to-customs pillar state that members should use a risk-management system to target and identify potentially high-risk cargo. Under these standards, members should also require advanced electronic information on container shipments to determine the risk posed by cargo. Further, member customs administrations should provide for joint targeting and screening, the use of standardized sets of targeting criteria, and compatible communication and information-exchange mechanisms. The customs-to-business pillar of the SAFE Framework incorporates the concept of the Authorized Economic Operator (AEO) and provides technical guidance for customs administrations to develop an AEO program that offers incentives to supply chain companies that comply with predetermined minimum security standards.¹⁵ In the United States, C-TPAT is the designated AEO program (and businesses participating in the program are Authorized Economic Operators). Just as in the C-TPAT program, the WCO customs-to-business pillar provides that the customs administration should, with representatives from the trade community, design a validation process for the respective AEO program that offers incentives to participating businesses. Further, the technical guidance for AEO programs states that participating businesses should develop mechanisms for the education and training of personnel regarding security practices. In essence, the SAFE Framework internationalizes the core principles of the CSI and C-TPAT programs.

According to the WCO, SAFE Framework stakeholders receive benefits from incorporating the core principles of the framework and implementing the standards. CBP officials stated that widespread implementation of the SAFE Framework benefits global container cargo security by shifting the focus of international customs administrations from primarily revenue collection to include enhanced security. Further, the SAFE Framework strengthens cooperation between customs administrations to improve their capability to detect high-risk cargo. Additionally, widespread implementation of the SAFE Framework could potentially help prevent

¹⁵ Authorized Economic Operators include, for example, manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, and distributors. Incentives for businesses participating in AEO programs are defined and offered by the individual member states. Some incentives could include (but are not limited to) expedited cargo release, access of information of value to AEO participants, special measures relating to periods of trade disruption or elevated threat levels, and first consideration for participation in any new cargo processing programs.

port shopping by terrorists or smugglers who look for seaports with more lax or nonexistent security standards. According to CBP and WCO officials, implementation of the SAFE Framework could benefit WCO member countries by enhancing security, speeding up operations, increasing revenue collection, and improving integrity programs for ensuring that customs administrations are free of corruption. The officials also noted that the SAFE Framework could lead to implementation of CSI-like customs security practices at non-CSI foreign seaports and enhance customs administration reform and modernization, which could improve the ability to detect high-risk cargo for antiterrorist security purposes. According to the WCO, the broad implementation of the standards also could allow companies to avoid the unnecessary burden of addressing different sets of requirements as a shipment moves through the supply chain logistics in different countries. Moreover, as we have previously reported, creating common standards facilitates collaboration between entities.¹⁶

Multiple Initiatives Are Under Way to Implement Elements of the SAFE Framework and to Promote Global Customs Security Standards

Working with the WCO and other international partners, CBP has taken several steps to support implementation of the SAFE Framework and to promote a customs environment that focuses on security. To help implement the SAFE Framework, CBP, along with the customs administrations of other countries, participates in a capacity-building program, known as the Columbus Program, which is coordinated through the WCO and fosters customs administration modernization in developing countries. Capacity-building activities consist of technical assistance and training, which lead to the establishment of infrastructure and procedures that are consistent with the objectives of the SAFE Framework standards. Capacity building consists of three phases: needs assessment, implementation, and monitoring. The first phase (needs assessment) provides an evaluation of a developing country's current capacity and existing gaps that would prevent it from implementing the SAFE Framework. The second phase (implementation) involves support from the assisting country to put into action recommendations derived from the needs assessment. Finally, the third phase involves monitoring the modernization practices put in place in phase two. According to the WCO, as of April 2008, 111 countries were participating in the capacity-building program. As of July 2008, 104 of these countries had completed the first

¹⁶GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

phase, 65 had moved into the second phase, and one was in the third phase. To carry out capacity-building activities, the WCO relies on contributions from individual donor countries like the United States. As a participating customs administration, CBP has provided training and assistance to 10 countries in the capacity-building program by developing customs regimes in these countries that incorporate the core elements of U.S. supply chain security programs, and thus the SAFE Framework. CBP has provided border enforcement training, integrity awareness training, and an advisory program. Additionally, CBP works with Asia-Pacific Economic Cooperation (APEC) member countries to help implement the WCO SAFE Framework through APEC's Framework for Secure Trade, which, according to CBP, is substantially identical to the WCO SAFE Framework.¹⁷ The APEC Framework enables member countries to advocate the implementation of the WCO SAFE Framework in non-WCO customs administrations, such as Taiwan.

In addition to working collaboratively with the international community to develop and implement the SAFE Framework, CBP has influenced the development of customs security practices in other countries through its own cargo security strategy. According to European customs administration officials we spoke to, the CSI program is beneficial because it provides a model for how to incorporate elements of the SAFE Framework, including targeting and the use of advance information, into their own customs practices. For example, the European Union recently amended its customs code to incorporate programs similar to CSI and C-TPAT.¹⁸ To further promote international supply chain security, since 2004, CBP has held an annual CSI global conference to share information on challenges met and best practices for customs operations. For example, in the August 2007 conference, two sessions specifically focused on

¹⁷APEC's purpose is to facilitate growth, trade, cooperation, and investment in the Asia-Pacific region. The APEC member countries are Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Republic of the Philippines, the Russian Federation, Singapore, Taiwan (Chinese Taipei), Thailand, United States of America, and Viet Nam.

¹⁸The Community Customs Code codifies European Community customs law. In May 2005, the European Parliament and the Council of the European Union adopted a regulation to amend the Community Customs Code. This amendment introduced measures that include (1) the use of a risk-management framework that is to be fully computerized by 2009, (2) the development of an Authorized Economic Operator program that entered into force on January 1, 2008, and (3) the mandatory requirement of advance electronic information on goods brought into or out of the European Union by July 1, 2009.

challenges encountered with capacity building and on best practices for CSI seaport operations. Additionally, the conference provided a forum for senior-level customs officials from all CSI countries to establish working relationships with one another and discuss future policy actions.

Just as the CSI program has influenced the ability of foreign customs administrations to target and examine high-risk containers in other countries, the C-TPAT program has helped influence the development of AEO programs. According to CBP officials as well as customs officials from Europe, Asia and Africa, operation of the C-TPAT program has provided a guide on how these programs should be operated. According to data from the WCO, about 70 countries have begun developing their own national AEO programs, which is essential to implementation of the SAFE Framework. Canada, Japan, Jordan, New Zealand, and Singapore have operational AEO programs in place. Other countries, such as Australia and some European Union nations will soon have operational systems in place. Further, through the WCO capacity-building program, several countries in the developing world have begun work on AEO pilots. For example, the East African Community—a regional intergovernmental organization made up of Burundi, Kenya, Rwanda, Tanzania, and Uganda—has started a program based on the SAFE Framework, which used the C-TPAT program as a model. Similarly, the Southern African Customs Union—made up of Botswana, Lesotho, Namibia, South Africa, and Swaziland—has also begun work on developing a pilot AEO program. Panama and Paraguay are considering AEO pilots as well.

CBP and International Partners Are Working to Achieve Mutual Recognition of Customs Security Practices

The SAFE Framework calls for a system of mutual recognition, and CBP has developed action plans and pilot programs to help develop mutual recognition relationships with other countries. There are two types of mutual recognition—first, the arrangement whereby the actions or decisions taken by one customs administration are recognized and accepted another administration and, second, an arrangement whereby the two nations’ AEO programs are mutually recognized by the respective customs administrations.¹⁹ CBP and other international customs officials see mutual recognition as providing an exit strategy for the CSI program (which includes reassigning or repatriating CBP officers stationed abroad) in some countries, as well as being a driver for further implementation of AEO programs. Finally, CBP engages in activities to assist in the development of a system of mutual recognition, such as pilot programs, and in June 2007, CBP signed a mutual recognition arrangement with New Zealand—the first ever such arrangement in the world—to recognize each other’s customs-to-business partnership programs.

CBP and International Organizations Have Defined Different Types of Mutual Recognition

CBP has worked with the international customs community to develop and implement the SAFE Framework, a set of international customs standards that calls for a system of mutual recognition, which the CBP and the WCO define as the arrangement whereby the actions or decisions taken by the customs administration of one country are recognized and accepted by the administration of another. Further, according to the WCO, for a system of mutual recognition to work, there must be an agreed-upon common set of standards that are applied in a uniform manner so that a level of confidence is possible between different customs administrations. The WCO distinguishes between mutual recognition of customs controls and mutual recognition of AEO programs, as described below and illustrated in figure 6.

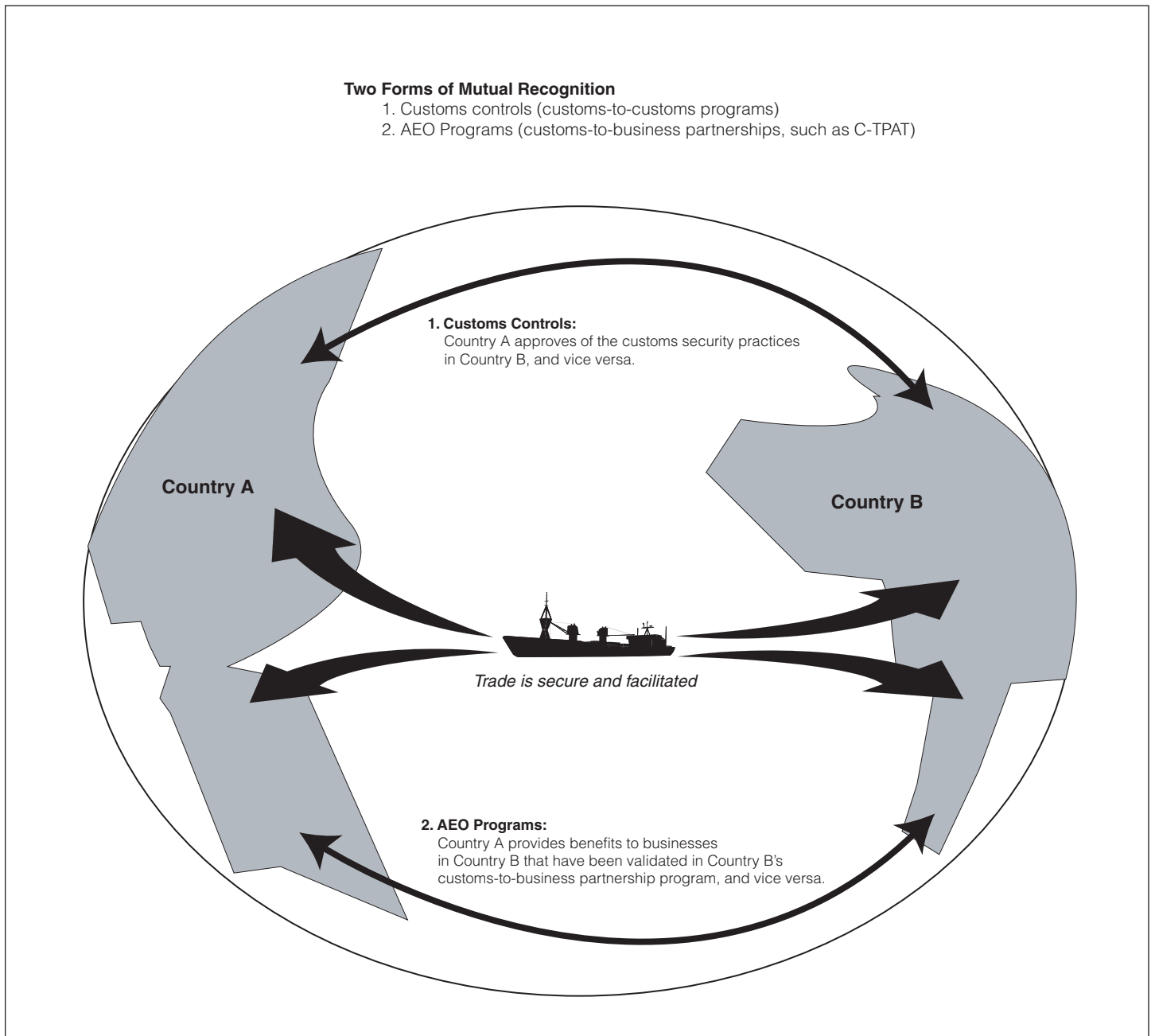
- Mutual recognition of customs controls is achieved when, for example, the customs administrations of two countries have confidence in each other’s procedures for targeting and inspecting cargo shipped in containers. According to the WCO, such mutual recognition could be

¹⁹Customs controls are the measures applied by the customs administration to ensure compliance with customs law. According to the revised Kyoto Convention (a WCO instrument), all goods that enter or leave a customs territory are subject to customs controls, and a customs administration should use risk management in the control of those goods exiting or entering the country. Therefore, all risk-management activities in customs, such as targeting and inspecting cargo, are considered customs controls.

achieved through joint targeting and screening, the use of standardized sets of criteria for identifying high-risk cargo for inspection, and compatible communication and information-exchange mechanisms.

- Mutual recognition of AEO programs 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.

Figure 6: Two Forms of Mutual Recognition



Source: GAO analysis and Art Explosion images.

The SAFE Framework states that members should work with each other to develop mechanisms for mutual recognition of customs controls and of AEO programs.

While CBP officials stated that the agency accepts the WCO definition of mutual recognition, CBP focuses its efforts and offers a process for achieving mutual recognition of AEO programs. CBP does not offer specific guidance on how to achieve mutual recognition of customs controls because officials believe that mutual recognition of AEO programs, such as the United States' C-TPAT program and New Zealand's AEO program, called the Secure Export Scheme, implies mutual recognition of customs controls. This is because, when obtaining information on a foreign country's AEO program, CBP officials also review the targeting and customs practices of that country. Therefore, according to CBP, there is no need for additional guidance or efforts with regard to mutual recognition of customs controls. However, an official from the WCO Private Sector Consultative Group (consisting of trade community partners from diverse industry and transport sectors) stated that there needs to be more clarity between the two types of mutual recognition and the benefits associated with each. CBP and WCO officials have stated that achieving mutual recognition of customs controls presents a challenge to customs administrations and may not be easily or quickly attained. According to those officials, this is because full recognition and adoption of the SAFE Framework does not by itself provide countries with confidence in each other's customs security practices and thus mutual recognition.

CBP and International Officials See Mutual Recognition as an Exit Strategy for the CSI Program in Some Countries and a Catalyst for Implementation of AEO Programs

CBP and European customs officials we spoke with see the benefit of mutual recognition as providing an exit strategy for the CSI program in some countries and being a catalyst for further implementation of AEO programs. CBP officials have stated that it was never the intention of the agency to keep CBP officers in foreign seaports under the CSI program indefinitely, but that a certain level of trust about the security practices of the customs administration of a foreign country and a common set of standards (i.e., mutual recognition) would be needed before CBP personnel at CSI seaports could be shifted to areas of greater need.

While the CSI program constitutes an effort to implement the SAFE Framework, it differs from the SAFE Framework in that it is a reciprocal program. The SAFE Framework calls for a system of mutual recognition between the customs administrations of two countries, whereas CSI requires CBP officers to be placed in foreign ports, and in return for

accepting the CSI program in a foreign country, the United States offers host countries the opportunity to place their customs officers in U.S. seaports to target oceangoing, containerized cargo being exported to their countries. However, when partner countries do not place their customs officers in a U.S. seaport, the CSI program focuses on identifying high-risk U.S.-bound containers at the CSI seaports (i.e., U.S. imports) and not on those containers outbound from the United States to foreign countries (i.e., U.S. exports). Alternatively, under a system of mutual recognition, in which comparable risk management principles are used, joint activities such as identifying cargo for inspection and cooperation between customs administrations would not require the placement of customs officials in foreign seaports. Further, the SAFE Framework requires that all countries inspect outbound high-risk containers at the request of the importing country if such a request is deemed to be reasonable. While the CSI program offers participating countries the ability to station their customs officials in U.S. seaports, 2 of the 33 countries participating in CSI—Canada and Japan—had decided to do so as of July 2008. Thus, the program primarily benefits U.S. security. European customs administration officials we spoke to stated that if all countries practiced reciprocity, as envisioned in the CSI program, each seaport would have numerous customs officials present from different countries, which is an inefficient use of resources. Alternatively, they said that implementation of a system of mutual recognition whereby customs officials in the United States have confidence that the customs controls and AEO programs of another country provided an acceptable level of security would be a more efficient use of limited resources.

CBP and customs officials we spoke to from Asia, Europe, and the South Pacific support mutual recognition of AEO programs. The WCO and industry representatives have stated that mutual recognition is an important benefit of AEO programs and will be the driving force behind further implementation of such programs internationally. Further, these officials stated that, in the absence of mutual recognition, there is little incentive for private companies to join AEO programs and, therefore, countries may not adopt this risk-management approach. Conversely, mutual-recognition systems provide some assurance that joining an AEO program could provide benefits across countries. According to CBP and the WCO, mutual recognition of AEO programs could reduce the need for multiple assessments of private sector supply chain firms by the customs administrations of different countries and could generate benefits for both industry and government—benefits that include faster clearances, reduced examinations, and rapid business resumption in the aftermath of a terrorist event.

CBP Has Engaged in Activities to Achieve Mutual Recognition with International Partners

CBP has been working to promote the SAFE Framework and engaging in pilot programs with foreign governments to harmonize customs efforts and to facilitate progress towards mutual recognition. For example, CBP is working with the European Commission—the executive arm of the EU—to standardize customs practices across countries to be consistent with the SAFE Framework. CBP and the European Commission’s Taxation and Customs Union Directorate, working through the Joint Customs Cooperation Committee, developed a 10-point action plan to further harmonize the customs efforts of the United States and the European Union.²⁰ This action plan includes the establishment of common data elements to be used for risk determination and a mechanism for the exchange of information, both of which are suggested by the SAFE Framework to assist in the development of mutual recognition of customs controls. The action plan also calls for a pilot to compare the United States’ C-TPAT program with the European Union’s AEO program for the purpose of achieving mutual recognition between the respective programs.²¹ Based on the 10-point action plan, CBP and the European Commission are also conducting a CSI pilot involving low-volume European seaports, known as the feeder port pilot program.²² Under the pilot, local customs officials at the feeder ports work with CBP officers located at CSI seaports to assess the risk and jointly determine whether the U.S.-bound container cargo originating in these feeder ports should receive further scrutiny. Local customs officials at the feeder seaports then inspect those U.S.-bound containers determined to be high risk before they are loaded on vessels at the feeder port. According to EU officials, the aim of coordinating on the efforts included in the 10-point action plan is to reduce the number of requirements that differ between European countries and the United States. Once these efforts are finalized, the EU intends to expand the projects to include other international partners. Table 2 describes elements of the 10-point action plan.

²⁰The U.S.-EU Joint Customs Cooperation Committee is co-chaired by the CBP Commissioner and the Director General of the European Commission’s Taxation and Customs Union Directorate and is responsible for overseeing all joint customs initiatives between CBP and the European Commission.

²¹The European Union’s AEO program became operational on January 1, 2008.

²²A feeder port is a port that ships cargo to a larger transit seaport.

Table 2: U.S.-EU Joint Customs Cooperation Committee Action Plan as of June 2008

Action item and description	Status
Conduct a transshipment pilot program – Pilot program to test security of and accuracy of information on transshipped cargo containers between the United States and the EU. ^a	Completed in 2006.
Develop a joint risk rules set – Establishment of U.S.-EU joint rules set for container security to allow for shared identification of security threats.	Ongoing. CBP and the EU completed the draft rules set in 2006. Beginning in April 2008, EU Officers were stationed at the National Targeting Center-Cargo and have refined this draft rules set. The updated rules set is currently being programmed within CBP's Automated Targeting System-International for testing.
Establish minimum control standards – Establishment of control standards for the handling of high-risk containers suspected of containing terrorist-related materials.	Completed. Minimum control standards jointly agreed to under the JCCC.
Develop a common list of advanced cargo data elements – Creation of a common list of cargo data elements that should be submitted in advance.	Completed in 2007.
Exchange information – Establishment of an exchange of information between the United States and the EU using the EU's secure Web site.	Completed 2007. CBP and the EU continue to exchange information through various mechanisms in accordance with the U.S.-EU Customs Mutual Assistance Agreement.
Conduct mutual recognition pilot of C-TPAT and EU AEO programs – Explore the feasibility of establishing mutual recognition between United States and EU customs-to-business partnership programs (C-TPAT and Authorized Economic Operator).	A joint U.S./EU roadmap towards mutual recognition was adopted on March 6, 2008. CBP and the European Commission will work to implement the roadmap and achieve mutual recognition of C-TPAT and the EU AEO in 2009.
Conduct a CSI feeder port pilot ^b – Pilot program to expand the reach of CSI by identifying the risk level of containers in feeder seaports at neighboring CSI seaports and having the examination, if needed, take place at the feeder port.	A 6-month pilot project was conducted at the Port of Szczecin, Poland, from March 2007 to September 2007. An evaluation of the pilot has been completed. In April 2008 the 6-month pilot commenced in the port of Aarhus, Denmark. A pilot with Salerno, Italy, is to begin in July 2008 and will also run for 6 months. Once all three pilots have been completed, further analysis will be conducted.
Conduct a joint threat assessment – The assessment summarizes the historical uses of weapons of mass effect as well as the present threat of such weapons to supply chain security. ^c	The joint threat assessment has been completed, although the United States and EU have agreed to an annual update. The update for 2008 was drafted and agreed to at the JCCC meeting in March 2008.
Station EU liaison officers at CBP's National Targeting Center–Cargo in Herndon, Va. – Is to provide for the stationing of EU Liaison officers at the National Targeting Center–Cargo to serve as point of contact with the EU and study centralized targeting operations. ^d	In order to provide an opportunity to gain an understanding of the work environment at the National Targeting Center-Cargo, EU customs officials were stationed at the center in April 2008. The first two (of a total of six) EU Officers were stationed at the NTC-C on April 14, 2008. The Officers have been working with CBP subject matter experts and rules developers to finalize and test the joint rules set as well as participating in various exchanges on topics of mutual interest. The next set of two representatives will deploy to the NTC-C on July 14, 2008.
Explore research and development Issues – Continuously explores areas for cooperation in the research and development field.	CBP and EU have agreed to keep one another abreast of ongoing research and development efforts and are exploring possible areas for cooperation.

Source: U.S. Customs and Border Protection and European Commission's Taxation and Customs Union Directorate.

^aTransshipment cargo containers are those that are unloaded from one ship to a seaport for a short period of time before being loaded onto another ship.

^bThe JCCC Action Plan originally called this action item “Minimum Requirement for Container Security Initiative.” It later evolved into the feeder port pilot program.

^cWeapons of mass effect are weapons capable of inflicting grave destructive, psychological, and/or economic damage. These include chemical, biological, nuclear, radiological, or explosive weapons.

^dThe mission of the National Targeting Center–Cargo is to support CBP’s cargo targeting operations. According to CBP, the center was established in response to the need for proactive targeting aimed at preventing acts of terror and to seize, deter, and disrupt terrorists and implements of terror.

European Commission officials we spoke with stated that activities undertaken with CBP under the action plan are for the purpose of harmonizing customs efforts and facilitating progress toward achieving mutual recognition of customs controls. For example, the feeder port project is seen as a step toward mutual recognition as containers are examined at the feeder port with no CBP officers present. According to officials from the European Commission and other European customs officials, with the establishment of these common security practices, a state of mutual recognition of customs controls between the European Union and the United States would exist, and there would no longer be a need to have CBP personnel stationed at European seaports as part of the CSI program. However, both European Commission and CBP officials stated that several hurdles exist before personnel could be removed from these seaports, such as verification of inspection and targeting programs and activities.

In addition to the European Union, CBP has been pursuing mutual recognition of AEO programs with those countries that have developed programs. For example, in June 2007, CBP entered into its first mutual recognition arrangement—that is, CBP and the New Zealand Customs Service mutually recognized each other’s respective customs-to-business partnership program. Under the arrangement, CBP recognizes members of New Zealand’s AEO program (the Secure Export Scheme) and provides benefits to New Zealand companies validated by the Secure Export Scheme similar to those of C-TPAT members and vice versa. According to a senior New Zealand customs official, requirements for membership and validation in the nation’s Secure Export Scheme program have been adapted from the United States’ C-TPAT program. CBP later signed mutual recognition arrangements with Jordan and Canada in June 2008. Further, CBP and the European Commission have agreed to establish mutual recognition of customs-to-business partnership programs by early 2009. The specific details of how the participating countries’ customs administrations plan to implement the mutual recognition arrangement—such as what benefits, if any, should be allotted to members of other countries’ AEO programs—are in the process of being worked out. Finally,

CBP is also negotiating with Japan and Singapore to establish mutual recognition arrangements with the industry partnership programs of those countries.

To that end, CBP has developed an approach to achieving mutual recognition of AEO programs with international partners. Prior to pursuing mutual recognition, these partners must have (1) submitted a letter of intent to the WCO to implement the SAFE Framework, (2) developed their own AEO program to enhance security, and (3) shown a willingness to commit to a four-phase mutual recognition process. The four phases are

- phase 1: an evaluation process that includes a comparison of both nations' programs to determine the similarities, differences, gaps, and challenges;
- phase 2: an operational planning and testing phase to determine the specific approach to how mutual recognition will be achieved, including the development of a pilot program;
- phase 3: conducting the pilot that was developed in phase two; and
- phase 4: declaration of mutual recognition.

Appendix III provides an overview of CBP's collaborative efforts to enhance container security.

While Working to Internationalize Customs Security Standards, CBP and International Partners Report Challenges in Balancing These Efforts with Other Legal Requirements

CBP has been actively engaged in the development and implementation of international customs security standards; however, recent laws requiring 100 percent scanning of U.S.-bound container cargo at foreign seaports may affect worldwide adoption of these standards. As required by the SAFE Port Act, CBP is currently testing the feasibility of 100 percent scanning in a pilot program; and, while CBP has not yet completed the pilot program, the 9/11 Act requires 100 percent scanning of all U.S.-bound container cargo by 2012, with possible extensions for individual seaports where specified conditions could hinder implementation. CBP and international partners also report facing challenges in implementing a 100 percent scanning requirement while also maintaining their risk-management security approach.

Recent Law to Improve Maritime Security Imposes New Requirements to Scan 100 Percent of U.S.-Bound Container Cargo

The SAFE Port Act of 2006 requires DHS to test the feasibility of 100 percent scanning of U.S.-bound containers. To fulfill this requirement, in December 2006, CBP and DOE jointly announced the formation of the Secure Freight Initiative. This initiative included the SFI pilot program, which became operational in October 2007. For more details on SFI, see appendix IV. While the SFI pilot project is still under way, the 9/11 Act was enacted. The act requires by 2012 100 percent scanning of all U.S.-bound container cargo using nonintrusive inspection equipment, including imaging equipment, which may use X-rays or gamma rays to create images of the containers' contents and radiation detection equipment at foreign seaports. The act also (1) specifies conditions for potential extensions beyond 2012 if a seaport cannot meet that deadline,²³ (2) requires DHS to develop technological and operational standards for scanning systems used to conduct 100 percent scanning at foreign seaports, and (3) requires DHS to ensure that actions taken under these provisions of the act do not violate international trade obligations and are consistent with the WCO SAFE framework or other international obligations of the United States. These provisions of the 9/11 Act replace requirements of the SAFE Port Act that called for 100 percent scanning of container cargo before its arrival in the United States. While the SAFE Port Act stated that this should be done as soon as possible, the 9/11 Act specifies a deadline of 2012. According to senior CBP officials, requiring 100 percent scanning before having the results of the SFI pilot compromises the credibility of the agency with its international partners because those countries that agreed to partner with CBP on the SFI pilot did so with the understanding that the findings would drive further discussions regarding a logical path forward.

While we have not yet fully reviewed the implementation of the 100 percent scanning requirement, we have a number of preliminary observations based on visits to foreign seaports and on discussions with officials from CBP, foreign customs administrations, and trade

²³The act allows for a 2-year extension and an option for renewal of the extension for 2-year increments thereafter if foreign ports can demonstrate that at least two of the following conditions exist: (1) scanning equipment is not available for purchase and installation; (2) scanning systems do not have a sufficiently low false alarm rate; (3) scanning systems cannot be purchased, deployed, or operated at ports overseas, for example, if a port does not have the physical characteristics to install such a system; (4) scanning systems cannot be integrated into existing systems; (5) the use of such a scanning system would significantly impact trade flows; and (6) scanning systems do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

organizations regarding potential challenges CBP and others may face in implementing this requirement. We also testified in June 2008 on challenges associated with implementing the 100 percent scanning requirement.²⁴

CBP and International Partners Report Facing Challenges in Balancing the 100 Percent Scanning Requirement with Current International Risk-Management Security Practices, and Concerns Remain regarding the Impact on Resources, Trade, and Security

CBP may have difficulty implementing a 100 percent scanning requirement while also maintaining a risk-management security approach that it has developed with many international partners. Currently, under the CSI program, CBP uses automated targeting tools to identify containers that pose a risk for terrorism for further examination before being placed on vessels bound for the United States. As we have previously reported, risk management reduces the risk of possible terrorist attack to the nation by allocating resources to those areas of greatest risk and is an approach accepted throughout the federal government.²⁵ Further, international partners have expressed to DHS and Congress that 100 percent scanning runs counter to the SAFE Framework, which is based on risk-management principles. WCO officials are concerned that 100 percent scanning could have an adverse impact on several of the organization's core instruments, which include not only the SAFE Framework but also the Revised Kyoto Convention—an international customs agreement to which the European Commission, the United States, and 52 other nations, have acceded.²⁶ Moreover, CBP and WCO officials stated that some countries are reluctant to implement AEO programs since they believe such programs would not be necessary with 100 percent scanning. Industry officials also stated that some companies are reluctant to join AEO programs since one of the main benefits of membership, a reduced likelihood of examination, would no longer apply with 100 percent scanning.

CBP's international partners have raised concerns about the impact on resources, security, and the flow of commerce should the 100 percent scanning requirement take effect. As we testified in June 2008, additional resources—including increased staff, equipment, and infrastructure—would be necessary for implementing 100 percent scanning of U.S.-bound container cargo at foreign seaports, and it is unclear who would be

²⁴GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008).

²⁵GAO-08-533T.

²⁶Signatories of the Revised Kyoto Convention pledge to use risk management principles in customs controls.

responsible for the costs. Given this situation, officials from the European Commission and CBP stated that unless additional resources are made available, 100 percent scanning could not be accomplished. According to officials from CBP, WCO, and the European Commission, 100 percent scanning may actually provide a lower level of security than the current method of targeting and examination using risk-management methods. Officials from CBP and the European Commission stated that the risk-management approach directs resources to where they are most needed, whereas scanning 100 percent of containers is inefficient because it directs too many resources to one activity—scanning—and diminishes the focus on those container shipments that pose the highest risk. According to a senior WCO official, under the current risk-management system, customs officers review the scanned images of high-risk containers in a very thorough and detailed manner. However, if the officers must review scanned images of all containers, the reviews may not be as thorough because the officers could lose focus due to the sheer volume of work. If more officers are not assigned, scanned images may not be properly or thoroughly analyzed, leading to a degradation of security. Further, a European customs administration official reported that 100 percent scanning could have a negative impact on the flow of international commerce, which under the 9/11 Act may be grounds for granting a 2-year, renewable extension to the 100 percent scanning requirement at individual seaports. The official also added that the 100 percent scanning requirement would disproportionately affect trade with developing countries.

Concluding Observations

In large part because of the collaborative international efforts in which CBP has taken a lead role, the global customs environment for ensuring supply chain security is significantly transforming. CBP is working in the international community actively and conscientiously to promote the adoption and implementation of global security standards for customs controls and for the adoption of AEO programs. Further, CBP has promoted a vision of mutual recognition whereby countries can have confidence in their respective customs security practices. To date, CBP has made substantial progress in working with foreign governments to develop and implement security practices based on components of CBP's CSI and C-TPAT programs. These efforts potentially point to an exit strategy for the CSI program in some countries and the generally more efficient use of all countries' resources through cooperative international relationships from the public and private sectors.

The transformation of customs security strategies from inward-looking programs to outward-looking and internationally cooperative relationships is in its early stages. While CBP has made progress developing global security initiatives, the agency faces challenges that may make it difficult to promote widespread adoption of a system of internationally accepted customs security standards and mutual recognition. In particular, significant challenges are posed by prospective implementation of the statutory provision that calls for 100 percent scanning of U.S.-bound container cargo at foreign seaports. Because of cost and logistical concerns, this provision may dissuade foreign governments and businesses from participating in risk-management security initiatives such as the CSI or C-TPAT programs as well as discourage other nations from developing their own AEO programs.

Agency Comments

We provided a draft of this report to the Department of Homeland Security and the Department of State for review and comment. The Department of Homeland Security provided technical comments, which we incorporated in this report where appropriate. The Department of State did not provide comments.

We are sending copies of this report to appropriate congressional committees, the Secretary of Homeland Security, and the Secretary of State. This report will also be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, 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. Key contributors to this report are listed in appendix V.



Stephen L. Caldwell
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable Daniel K. Inouye
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Carl Levin
Chairman
The Honorable Norm Coleman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable John D. Dingell
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Ted Stevens
United States Senate

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from the Chairman and Vice Chairman, Senate Committee on Commerce, Science, and Transportation; the Chairman and Ranking Member, Senate Committee on Homeland Security and Governmental Affairs; the Chairman and Ranking Member, Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs; and the Chairman, House Committee on Energy and Commerce, we reviewed U.S. Customs and Border Protection's (CBP) programs—the Container Security Initiative (CSI) program and the Customs-Trade Partnership Against Terrorism (C-TPAT) program—and CBP's efforts to promote international supply chain security standards. For this report, our review focused on the following questions regarding CBP's efforts to promote and implement an international framework of standards for supply chain security:

- What actions has CBP taken to develop and implement international supply chain security standards?
- What actions has CBP taken with international partners to achieve mutual recognition of customs security practices?
- What issues do CBP and foreign customs administrations working to internationalize customs security standards anticipate in implementing 100 percent scanning of U.S.-bound container cargo?

Scope and Methodology

In reviewing CBP's CSI program, C-TPAT program, and international initiatives in supply chain security, we are releasing three reports—one on the CSI program issued in January 2008, one on the C-TPAT program issued in April 2008, and this report on CBP's international supply chain security initiatives.¹ We conducted this performance audit in conjunction with concurrent reviews of the CSI and C-TPAT programs from May 2006 to July 2008. To determine what actions CBP has taken and its role in developing and implementing international supply chain security standards, we met with officials at CBP's Office of International Affairs and Trade Relations and the Office of Field Operations to discuss the

¹See GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, [GAO-08-187](#) (Washington, D.C.: Jan. 25, 2008), and *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, [GAO-08-240](#) (Washington, D.C.: Apr. 25, 2008). Also, see GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, [GAO-08-533T](#) (Washington, D.C.: June 12, 2008).

issues within the scope of this review. We reviewed the strategic plans of the CSI and C-TPAT programs. We also reviewed CBP documents related to its participation in capacity-building efforts. Further, we attended CBP's 2007 CSI Global Targeters Conference that took place in Arlington, Virginia, from August 28 to 30, 2007. The conference brought together, among others, foreign customs officials from participating CSI countries and CBP officials stationed at CSI seaports and from headquarters and provided a forum for sharing challenges met and best practices for CSI country participants. At the conference, we gathered information and spoke with officials involved in many aspects of the international customs arena. To determine CBP's role in the development of the World Customs Organization's (WCO) SAFE Framework of Standards to Secure and Facilitate Global Trade (more commonly referred to as the SAFE Framework), we reviewed the meeting minutes and reports from the WCO's High Level Strategic Group, the group tasked with developing the principles and standards of the SAFE Framework. These meeting notes helped us determine CBP's participation in the development of these standards. We also reviewed the SAFE Framework itself. Additionally, we spoke with WCO officials in Brussels. We reviewed WCO documents related to capacity-building efforts and progress towards implementation of the SAFE Framework.

We also visited 6 of the 58 CSI seaports. CSI seaports operate in 33 countries, and we selected these six CSI seaports based on geographic and strategic significance, container volume to the United States from the seaports, when the seaports began conducting CSI operations, and whether the seaport was involved in CBP's Secure Freight Initiative. The results from our visits to seaports provided examples of CBP and host government operations but cannot be generalized beyond the seaports visited because we did not use statistical sampling techniques in selecting the seaports.

We also spoke with the European and Asian customs officials in foreign embassies in Washington, D.C. Further, we spoke with foreign customs officers stationed at the Port of Long Beach, California, as part of the reciprocal agreement of the CSI program. While the perspectives of foreign officials we spoke to cannot be generalized across the wider population of countries, they provided us an overall understanding of how CBP interacts with foreign customs officials at overseas seaports. To determine CBP's role in implementing the SAFE Framework in the Asian-Pacific region, we reviewed meeting reports from the Asia-Pacific Economic Cooperation's Subcommittee on Customs Procedures.

Regarding the second and third questions—that is, CBP’s efforts in achieving mutual recognition of customs practices and business partnership programs and the challenges CBP faces as it moves forward with its international supply chain security initiatives—we spoke with the European Union’s European Commission officials in the United States and with the European Commission’s Taxation and Customs Union Directorate and the Transportation and Energy Directorate, both located in Brussels, Belgium. We reviewed meeting notes and reports from the U.S.-EU Joint Customs Cooperation Committee and official agreements between the United States and the EU. We also spoke with officials from the customs administration of New Zealand, the first country with which the United States has a mutual recognition arrangement, and reviewed the official arrangement between the two countries. We further reviewed official documents from CBP and the WCO regarding mutual recognition. We attended the WCO World Customs Forum 2007, an international conference on the SAFE Framework that took place at WCO headquarters in Brussels, Belgium, on December 11 and 12, 2007. The forum provided a critical implementation review of the SAFE Framework, including the development of customs-to-business partnership programs, mutual recognition efforts, and obstacles preventing widespread implementation of international standards and programs. It also brought together recognized experts in global trade, supply chain security, international trade law, and customs procedures. We also spoke with members of industry organizations including CBP’s Departmental Advisory Committee on Commercial Operations and the Federation of European Private Port Operators.² Additionally, we spoke with the private terminal operators at the six CSI seaports we visited as well as with officials from the port authorities. At the CSI seaports, we interviewed host government officials and observed conditions at the seaports regarding the scanning of containers. Finally, we reviewed recent U.S. legislation dealing with maritime security, in particular the Security and Accountability for Every Port Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act of 2007.

²CBP’s Departmental Advisory Committee on Commercial Operations was established by the Omnibus Budget Reconciliation Act of 1987 to advise the Secretaries of the Department of the Treasury and the DHS on the commercial operations of CBP and related DHS and Treasury functions. The Federation of European Private Port Operators is a private industry organization representing the interests of about 800 private port operators in Europe.

We conducted this performance audit from May 2006 through July 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: World Customs Organization SAFE Framework of Standards

The World Customs Organization Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework) is built on the twin pillars of the customs-to-customs network arrangements and the customs-to-business partnerships. Table 3 describes the 11 standards that govern the interaction between the customs administrations of different countries in the customs-to-customs pillar, and table 4 describes the 6 standards that govern the interactions between a customs administration and the businesses participating in commercial trade activities through various supply chains in the customs-to-business pillar.

**Appendix II: World Customs Organization
SAFE Framework of Standards**

Table 3: WCO SAFE Framework—Standards for the Customs-to-Customs Pillar

Standard	Title	Description
1	Integrated Supply Chain Management	The Customs administration should follow integrated customs controls procedures as outlined in the WCO Customs Guidelines on Integrated Supply Chain Management.
2	Cargo Inspection Authority	The customs administration should have the authority to inspect cargo originating, exiting, transiting (including remaining on board), or being transhipped through a country.
3	Modern Technology Inspection Equipment	Nonintrusive inspection equipment and radiation detection equipment should be available and used for conducting inspections, where available and in accordance with risk assessment. This equipment is necessary to inspect high-risk containers or cargo quickly, without disrupting the flow of legitimate trade.
4	Risk-Management Systems	The customs administration should establish a risk-management system to identify potentially high-risk shipments and automate that system. The system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices.
5	High-Risk Cargo or Container	High-risk cargo and container shipments are those for which there is inadequate information to deem shipments as low risk, that tactical intelligence indicates as high risk, or that a risk-scoring assessment methodology based on security-related data elements identifies the shipment as high risk.
6	Advance Electronic Information	The customs administration should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place.
7	Targeting and Communication	The customs administration should provide for joint targeting and screening, the use of standardized sets of targeting criteria, and compatible communication and/or information exchange mechanisms; these elements will assist in the future development of a system of mutual recognition of controls.
8	Performance Measures	The customs administration should maintain statistical reports that contain performance measures including, but not limited to, the number of shipments reviewed, the subset of high-risk shipments, examinations of high-risk shipments conducted, examinations of high-risk shipments by nonintrusive inspection technology, examinations of high-risk shipments by nonintrusive inspection and physical means, examinations of high-risk shipments by physical means only, and customs clearance times and positive and negative results. Those reports should be consolidated by the WCO.
9	Security Assessments	The customs administration should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and commit to resolving identified gaps expeditiously.
10	Employee Integrity	The customs administration and other competent authorities should be encouraged to require programs to prevent lapses in employee integrity and to identify and combat breaches in integrity.
11	Outbound Security Inspections	The customs administration should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.

Source: World Customs Organization.

**Appendix II: World Customs Organization
SAFE Framework of Standards**

Table 4: WCO SAFE Framework—Standards for the Customs-to-Business Pillar

Standard	Title	Description
1	Partnership	Authorized Economic Operators involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments and containers until they are released from customs controls at destination.
2	Security	Authorized Economic Operators will incorporate pre-determined security best practices into their existing business practices.
3	Authorization	The customs administration, together with representatives from the trade community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as Authorized Economic Operators.
4	Technology	All parties will maintain cargo and container integrity by facilitating the use of modern technology.
5	Communication	The customs administration will regularly update customs-business partnership programs to promote minimum security standards and supply chain security best practices.
6	Facilitation	The customs administration will work co-operatively with Authorized Economic Operators to maximize security and facilitation of the international trade supply chain originating in or moving through the administration's customs territory.

Source: World Customs Organization.

Appendix III: CBP's Collaborative Efforts to Enhance Container Security

CBP has collaborated with several partners or working groups to enhance international container security. Some of these partners or groups include the World Customs Organization (WCO), the Asia-Pacific Economic Cooperation (APEC), member countries and the customs administrations of the European Union, the New Zealand Customs Service, and the Canada Border Services Agency. Table 5 describes some of the collaborative work done by CBP.

Table 5: CBP's Collaborative Efforts to Enhance Container Security

Partner or working group	Purpose of working group	Status of working group efforts as of June 2007 UPDATE
WCO High Level Strategic Group	Prepare a framework for security and facilitation of the global supply chain. Provide high-level guidance on implementation and development issues.	<ul style="list-style-type: none"> Formulated, adopted, and began implementation of the WCO Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework). Began work on capacity building. Sunset in June 2007.
WCO SAFE Working Group	Monitor, maintain, and develop the WCO Framework.	<ul style="list-style-type: none"> Established June 2007 by WCO Council. The first meeting concluded in October 2007 (Brussels, Belgium) and the second meeting was held April 22 to 23, 2008. The primary focus of this meeting was the security filing requirements and refining the SAFE Working Group Operations. CBP also provided an update on the status of the 100% scanning law and SFI pilot projects.
U.S.-EU Joint Customs Cooperation Committee (JCCC)	The U.S.-EU JCCC was established under the Customs Cooperation and Mutual Assistance in Customs Matters agreement signed May 28, 1997, to collaborate on customs issues.	<ul style="list-style-type: none"> Under the April 22, 2004, agreement to intensify and broaden the existing Customs Cooperation and Mutual Assistance in Customs Matters agreement, the JCCC was assigned oversight of a working-level expert group on container security and supply chain security issues. See status of working group below under U.S.-EU JCCC Steering Committee.

Appendix III: CBP's Collaborative Efforts to Enhance Container Security

Partner or working group	Purpose of working group	Status of working group efforts as of June 2007 UPDATE
U.S.-EU JCCC Steering Committee	<p>Was established to carry out the following U.S.-EU JCCC initiatives:</p> <ul style="list-style-type: none"> • Establishment of CSI Minimum Requirements/CSI Feeder Port Pilot. • Establishment of Minimum Control Standards for the inspection of high-risk cargo. • Establishment of a Joint Threat Assessment. • Creation of a Joint Risk Rules Set. • Creation of one Common List of Data Elements. • Transshipment Pilot to test security of and accuracy of information on transshipped cargo between the U.S. and the EU. • Exchange of Information. • Stationing of EU Liaison Officers at the National Targeting Center-Cargo (NTC-C) in Herndon, Va. • Mutual Recognition of trade partnership programs. • Research and development Issues. 	<ul style="list-style-type: none"> • CSI Minimum Requirements/Feeder Port Pilot – Minimum Requirements jointly agreed to under the JCCC/CSI Feeder Port Pilot - Feeder Port Pilots currently underway in 3 locations: Szczecin, Poland (complete); Aarhus, Denmark (operational); and Salerno, Italy (set to begin July 2008). • Minimum Control Standards – Action completed – minimum control standards jointly agreed to under the JCCC. • Joint Threat Assessment – Remains an ongoing action under the sharing of information and will be shared, as deemed appropriate, with the WCO. The update for 2008 was drafted and agreed to at the JCCC meeting in March 2008. The United States and EU have agreed to an annual update. • Joint Risk Rules – Set of rules drafted in 2006. They have been further developed and are currently being programmed and tested under the EU Liaison Officers action item. • Common List of Data Elements – Action Completed. • Transshipment Pilot – Action completed. • Exchange of Information – The U.S. and the EU continue to exchange information under the auspices of the U.S.-EU Customs Mutual Assistance Agreement. • EU Liaison Officers – The first two (of six total) EU Officers have been stationed at the NTC-C. • Mutual Recognition – Agreement of a road map toward mutual recognition between the United States and EU completed in March 2008. • R&D – Continuously exploring areas for cooperation in the R&D field.
Asia-Pacific Economic Cooperation (APEC) Sub-Committee on Customs Procedures	<p>To assist APEC member economies in adopting the APEC Framework for Secure Trade leading to the implementation of international standards for securing and facilitating the global supply chain.</p>	<ul style="list-style-type: none"> • As of April 2008, CBP had completed the last component of a three part seminar begun in July 2007—"Essential Legal Authorities," "Establishment of Industry Partnership Programs," and "Supply Chain Security Specialist Training," which was directed at supply chain specialists who would be directly involved in the operation of the program. • As APEC member economies move toward implementing AEO programs, CBP will continue to work with all economies to develop a methodology for mutual recognition of AEOs authorized by other member economies to avoid inconsistent, redundant and duplicative requirements and audits for AEOs. • CBP is actively engaged as the chair of the Collective Action Plan Evaluation Working Group.
CBP – New Zealand Customs Service Mutual Recognition Arrangement	<p>To further secure the supply chain between CBP and the New Zealand Customs Service.</p>	<ul style="list-style-type: none"> • In June 2007, CBP and the New Zealand Customs Service signed a Mutual Recognition Arrangement that recognizes the extension of comparable benefits among members of CBP's Customs-Trade Partnership Against Terrorism and the New Zealand Customs Service's Secure Export Scheme. The United States has discussed the benefits of a mutual recognition agreement with New Zealand. These include reduced inspections and the ability to reallocate customs resources in a more efficient fashion.

Appendix III: CBP's Collaborative Efforts to Enhance Container Security

Partner or working group	Purpose of working group	Status of working group efforts as of June 2007 UPDATE
CBP-Japan Customs & Tariff Bureau ("CTB") Mutual Recognition Arrangement Negotiations	To further secure the supply chain between CBP and the Japan Customs and Tariff Bureau.	<ul style="list-style-type: none"> • CBP and JCTB have completed the first phase of Mutual Recognition Arrangement negotiations, which was the successful completion of a comparative analysis between the two customs administrations' programs. As of July 2008, CBP and JCTB are currently planning joint validations of Japanese companies. CBP and JCTB look to sign an MRA by the end of the calendar year.
CBP – Jordan Mutual Recognition Arrangement	To further secure the supply chain between CBP and The Jordanian Customs Department.	<ul style="list-style-type: none"> • In June 2008, CBP and the Jordan Customs Department signed a mutual recognition arrangement that recognizes the extension of comparable benefits between members of C-TPAT and Jordan's Golden List Program. It is the first mutual recognition arrangement signed with a Middle Eastern nation.
CBP – Canada Border Services Agency Partnership	To further secure the supply chain between CBP and Canada Border Services Agency.	<ul style="list-style-type: none"> • In June 2008, CBP and the Canada Border Services Agency signed a mutual recognition arrangement that recognizes the extension of comparable benefits between members of C-TPAT and Canada's Partnership in Protection program.

Source: GAO presentation of information gathered from CBP.

Appendix IV: The Secure Freight Initiative

To improve maritime container security, the SAFE Port Act was enacted in October 2006 and requires, among other things, that CBP conduct a pilot program to determine the feasibility of scanning 100 percent of U.S.-bound containers. It also specifies that the pilot should test integrated scanning systems that combine the use of radiation portal monitors and nonintrusive inspection equipment, building upon CSI and the Megaports Initiative. To fulfill this and other requirements of the SAFE Port Act, CBP and DOE jointly announced the formation of the Secure Freight Initiative (SFI) in December 2006.

The goal of SFI is to build upon existing port security measures by enhancing the U.S. government's ability to scan containers for nuclear and radiological materials overseas and better assess the risk of U.S.-bound containers. According to CBP officials, SFI is to be rolled out in three phases. The initial phase is the International Container Security project—commonly known as the SFI pilot program. The SFI pilot program tests the feasibility of 100 percent scanning of U.S.-bound container cargo at six overseas seaports meant to represent a diverse array of trade processing capacities with varying container traffic contents and flows. The SFI pilot program involves the deployment of advanced cargo scanning capabilities and an integrated examination system to participating overseas ports. The advanced cargo scanning equipment—NII and radiation detection equipment—produce data to indicate the presence of illicit nuclear and radiological material in containers. The integrated examination system then uses software to make this information available to CBP for analysis. According to CBP, it will review the scan data at the foreign seaport or at CBP's National Targeting Center–Cargo (NTC-C) in the United States.¹ If the scanning equipment indicates a potential concern, both CSI and host government customs officials are to simultaneously receive an alert and the specific container is to be further inspected before it continues on to the United States.

Table 6 lists the seaports participating in the SFI pilot program. As shown in the table, three SFI seaports are to scan 100 percent of U.S.-bound

¹According to CBP, the National Targeting Center (NTC) was established in response to the need for proactive targeting aimed at preventing acts of terror and to seize, deter, and disrupt terrorists and implements of terror. NTC originally combined both passenger and cargo targeting in one facility. It was later divided into NTCC and the National Targeting Center–Passenger. For purposes of this report, we use NTCC in our references since its mission is to support CBP cargo-targeting operations.

container cargo that passes through those seaports, while the other three seaports are to deploy scanning equipment in a more limited capacity.

Table 6: Information on the Six Foreign Seaports Participating in the SFI Pilot Program

SFI port	Deployment level when pilot operational	Testing date ^a	Operational date ^b	Volume of U.S.-bound containers, fiscal year 2007
Qasim, Pakistan	Full ^c	March 31, 2007	October 12, 2007	7,295
Puerto Cortez, Honduras	Full ^c	April 2, 2007	October 12, 2007	75,800
Southampton, UK	Full ^c	August 23, 2007	October 12, 2007	25,627
Hong Kong	Limited ^d	November 19, 2007	January 11, 2008	795,138
Busan, South Korea	Limited ^d	June 8, 2008	September 2008 (projected)	645,467
Salalah, Oman	Limited ^d	August 2008 (projected)	September 2008 (projected)	45,997

Source: U.S. Customs and Border Protection.

^aTesting date is defined as the date when the scanning systems are in place and operational testing begins.

^bOperational date is defined as the date when the SFI scanning data are transmitted successfully to the local central alarm station and to the CBP network in the United States.

^cFully operational seaports are to scan 100 percent of U.S.-bound container cargo under the SFI pilot program.

^dLimited operation seaports are to scan less than 100 percent of U.S.-bound container cargo. For these seaports, CBP plans to conduct SFI operations at a reduced level, typically limited to one terminal in the port, such as Gamman Terminal in Busan.

Phase two of SFI is the implementation of a requirement that importers and cargo carriers provide certain additional information about the cargo they are transporting to the United States prior to loading at the foreign port. The additional information will allow CBP to better target high-risk cargo. In general, this security filing—also called “10+2”—requires importers to provide data elements that further identify the entities involved in the supply chain and their locations as well as a more precise identification of the items shipped to the United States. CBP worked with its Departmental Advisory Committee on Commercial Operations and the trade community to identify the specific data elements to be required, which resulted in the 10+2 additional data elements required. CBP published a notice for proposed rulemaking in the Federal Register on the 10+2 security filing in January 2008, and the regulations underwent a public comment period until March 2008. This phase is currently in the development stage.

As required by the SAFE Port Act, CBP issued a report in June 2008 on the lessons learned from the SFI pilot program and the need and feasibility of expanding the 100 percent scanning system to other CSI seaports, among other things.² Every 6 months after the issuance of this report, CBP is to report on the status of full-scale deployment of the integrated scanning systems at foreign seaports to scan 100 percent of U.S.-bound cargo.

²6 U.S.C. § 981(d). The DHS Appropriations Act for fiscal year 2007, enacted shortly before the SAFE Port Act, also required a pilot program to test 100 percent scanning at three ports, and established similar, but not identical, requirements for the program. For example, the report to Congress on lessons learned is to include a plan and schedule to expand the scanning system developed under the pilot to other CSI ports rather than an assessment of the need and feasibility of such an expansion.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

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

Acknowledgments

In addition to the contact named above, Christine A. Fossett and Danny R. Burton, Assistant Directors, and Robert Rivas, Analyst-in-Charge, managed this assignment.

Stephanie Fain, Valerie Kasindi, Matthew Lee, and Leslie Sarapu made significant contributions to the work.

Stanley Kostyla assisted with design and methodology.

Frances Cook provided legal support.

Sally Williamson provided assistance in report preparation.

Pille Anvelt and Avy Ashery developed the report's graphics.

Related GAO Products

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

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. [GAO-08-126T](#). Washington, D.C.: October 30, 2007.

Maritime Security: One Year Later: A Progress Report on the SAFE Port Act. [GAO-08-171T](#). Washington, D.C.: October 16, 2007.

Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports. [GAO-08-86T](#). Washington, D.C.: October 4, 2007.

Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment. [GAO-07-1247T](#). Washington, D.C.: September 18, 2007.

Maritime Security: Observations on Selected Aspects of the SAFE Port Act. [GAO-07-754T](#). April 26, 2007.

Customs Revenue: Customs and Border Protection Needs to Improve Workforce Planning and Accountability. [GAO-07-529](#). Washington, D.C.: April 12, 2007.

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.

Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries. [GAO-05-840T](#). Washington, D.C.: June 21, 2005.

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.

Homeland Security: Key Cargo Security Programs Can Be Improved. [GAO-05-466T](#). Washington, D.C.: May 26, 2005.

Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges. [GAO-05-448T](#). Washington, D.C.: May 17, 2005.

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

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. [GAO-05-375](#). Washington, D.C.: March 31, 2005.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. [GAO-05-170](#). Washington, D.C.: January 14, 2005.

Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. [GAO-05-106](#). Washington, D.C.: December 10, 2004.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. [GAO-04-838](#). Washington, D.C.: June 30, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. [GAO-04-557T](#). Washington, D.C.: March 31, 2004.

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 Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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