

GAO

Report to the Chairman, Committee on
Homeland Security, House of
Representatives

September 2010

SUPPLY CHAIN SECURITY

DHS Should Test and
Evaluate Container
Security Technologies
Consistent with All
Identified Operational
Scenarios to Ensure
the Technologies Will
Function as Intended



GAO

Accountability * Integrity * Reliability

Why GAO Did This Study

Cargo containers could be used to transport unlawful cargo, including weapons of mass destruction, illicit arms, stowaways, and illegal narcotics into the United States. Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for container security. To enhance container security, CBP has partnered with DHS's Science and Technology (S&T) Directorate to develop performance standards—requirements that must be met by products to ensure they will function as intended—for container security technologies. After successful completion of testing, S&T plans to deliver performance standards to DHS's Office of Policy Development and CBP. As requested, this report addresses (1) the extent to which DHS has made progress in conducting research and development and defining performance standards for the technologies, and (2) the remaining steps and challenges, if any, DHS could face in implementing the technologies. GAO, among other things, reviewed master test plans for S&T's four ongoing container security technology projects, and interviewed DHS officials.

What GAO Recommends

GAO recommends that DHS test and evaluate the container security technologies consistent with all the operational scenarios DHS identified for potential implementation. DHS concurred with our recommendation.

View [GAO-10-887](#) or key components. For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov or Timothy Persons at (202) 512-6412 or personst@gao.gov.

SUPPLY CHAIN SECURITY

DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended

What GAO Found

DHS has conducted research and development for four container security technology projects, but has not yet developed performance standards for them. From 2004 through 2009, S&T spent approximately \$60 million and made varying levels of progress in the research and development of its four container security technology projects. These projects include the Advanced Container Security Device (ACSD), to detect intrusion on all six sides of a container; the Container Security Device (CSD), to detect the opening or removal of container doors; the Hybrid Composite Container, a lightweight container with an embedded sensor grid to detect intrusion on all six sides of the container; and the Marine Asset Tag Tracking System (MATTS), to track containers. The ACSD and Hybrid Composite Container technologies have not yet completed laboratory testing, but the CSD and MATTS are proceeding to testing in an operational environment, which will determine if the technologies can operate in the global supply chain—the flow of goods from manufacturers to retailers. S&T's master plans for conducting operational environment testing, however, do not reflect all of the operational scenarios the Office of Policy Development and CBP are considering for implementation. According to DHS guidance, before S&T can provide performance standards to the Office of Policy Development and CBP, the technologies are to have been proven to work in their final form and under expected operational conditions. Until the container security technologies are tested and evaluated consistent with all of the operational scenarios DHS identified for potential implementation, S&T cannot provide reasonable assurance that the technologies will effectively function as the Office of Policy Development and CBP intend to implement them.

If S&T determines that the container security technologies are mature enough to provide performance standards for these technologies to the Office of Policy Development and CBP, key steps and challenges remain before implementation can occur. These key steps involve (1) obtaining support from the trade industry and international partners, (2) developing a concept of operations (CONOPS) detailing how the technologies are to be deployed, and (3) certifying the technologies for use. The Office of Policy Development and CBP plan to take these steps if and when S&T provides performance standards.

Description of DHS S&T's Four Container Security Projects

Project name	Project description and goal
ACSD	Develop a device that can detect and report container intrusion on all six sides of a container.
CSD	Develop a device that can detect and report the opening or removal of container doors.
Hybrid Composite Container	Develop a composite container with embedded security sensors to detect intrusion on all six sides.
MATTS	Establish a system to track containers, and increase the range that CSDs and ACSDs can communicate.

Source: GAO analysis of DHS S&T information.

Contents

Letter		1
	Background	5
	DHS Has Made Progress in Researching and Developing Container Security Technologies, but Needs to Conduct Testing Using Defined Operational Scenarios before Delivering Performance Standards	16
	Key Steps and Challenges Remain before Implementation of Container Security Technologies Can Move Forward	27
	Conclusions	33
	Recommendation for Executive Action	34
	Agency Comments	34
Appendix I	Vendors Selected to Participate in Container Security Technology Projects	36
Appendix II	Description of Container Security Technologies' Communications Systems	37
Appendix III	Comments from the Department of Homeland Security	40
Appendix IV	GAO Contacts and Staff Acknowledgments	42
Glossary		43
Related GAO Products		47
Tables		
	Table 1: Description of CBP's Core Cargo Security Programs	9
	Table 2: Description of DHS S&T's Four Container Security Projects	14

Table 3: Members of the Container Security Test and Evaluation (CSTE) Team and Their Respective Roles and Responsibilities on the Container Security Technology Projects	17
Table 4: Status of Container Security Technology Projects	18
Table 5: Description of CSTE’s Testing of the ACSD Prototypes	20
Table 6: Description of CSTE’s Testing of the CSD Prototypes	22
Table 7: Selection and Funding of Vendors for Development of Container Security Technologies	36

Figures

Figure 1: The Maritime Supply Chain Process	6
Figure 2: Drawings of a Typical Cargo Container, Its Parts, and Dimensions	8
Figure 3: A Container Sealed with a Bolt Seal	12
Figure 4: DHS S&T Testing Process	15
Figure 5: Photographs of GTRI’s and SAIC’s Container Security Devices	23
Figure 6: Photograph of iControl, Inc.’s MATTS Tag	26
Figure 7: Certification Testing Process	33
Figure 8: Security Device System Supporting Container Security Technology Communications	38

Abbreviations

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ACSD	Advanced Container Security Device
BAA	broad agency announcement
C-TPAT	Customs-Trade Partnership Against Terrorism
CBP	Customs and Border Protection
CM	communications module
CONOPS	concept of operations
CSD	Container Security Device
CSI	Container Security Initiative
CSTE Team	Container Security Test and Evaluation Team
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
GTRI	Georgia Tech Research Institute
ISO	International Organization for Standardization
MATTS	Marine Asset Tag Tracking System
MSC	Maine Secure Composites
MTSA	Maritime Transportation Security Act of 2002
NII	non-intrusive inspection
RF	radio frequency
S&T	Science and Technology
SAFE Port Act	Security and Accountability for Every Port Act
SAIC	Science Applications International Corporation
SBIR	Small Business Innovative Research
SFI	Secure Freight Initiative
TEU	twenty-foot equivalent unit
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. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 29, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

In addition to serving an important role in transporting legitimate cargo, cargo containers can also be used to transport unlawful cargo, including weapons of mass destruction (WMD), illicit arms, stowaways, and illegal narcotics, into the United States. In fiscal year 2009, 9.8 million cargo containers arrived at U.S. ports. Within the federal government, the Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) is responsible for administering container security and reducing the vulnerabilities associated with the supply chain—the flow of goods from manufacturers to retailers. As it performs this mission, CBP maintains two overarching and sometimes conflicting goals—increasing security while efficiently facilitating legitimate trade. To address these goals, CBP has developed a layered security strategy.¹ Core components of this strategy include analyzing information to identify cargo containers that may pose a security risk, working with host governments to examine high-risk containers at foreign ports before they are loaded onto vessels bound for the United States, and providing benefits, such as reduced examination of cargo, to private-sector companies that comply with predetermined security measures.

Recognizing that security can be further enhanced, CBP has partnered with DHS's Science and Technology (S&T) Directorate to develop performance standards—requirements that must be met by products to ensure they will function as intended—for container security technologies

¹We have previously reviewed components of CBP's layered security strategy. See, for example, GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, [GAO-10-12](#) (Washington, D.C.: Oct. 30, 2009); *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).

that can (1) detect and report container intrusion, (2) alert officials to possible security threats, and (3) track the movement of cargo containers through the supply chain. S&T is responsible for researching, developing, testing, and evaluating new technologies in order to develop performance standards.² If S&T is able to demonstrate through testing and evaluation that container security technologies exist that can meet CBP's requirements, then it plans to provide performance standards to CBP and the Transportation, Cargo & Infrastructure Unit within DHS's Office of Policy Development to pursue for implementation.³ The Transportation, Cargo & Infrastructure Unit is responsible for, among other things, developing, implementing, and coordinating policy relating to the security of the global supply chain.

You requested information on DHS's efforts to develop and implement container security technologies. In particular, this report addresses the following questions:

- To what extent has DHS made progress in conducting research and development and defining performance standards for container security technologies?
- What remaining steps and challenges, if any, does DHS face in implementing container security technologies?

To address the first objective, we reviewed all four ongoing container security projects initiated by S&T to develop technologies that can detect cargo container intrusions and track the movement of cargo containers through the supply chain. For each of the four projects, we reviewed project requirements documents, test plans, technology transition agreements, and task orders to determine the projects' scope and requirements. We then evaluated DHS's plans against criteria for planning in DHS's *Developing Operational Requirements* guide.⁴ To assess DHS's progress in developing technologies, we reviewed the test reports

²The container security technology projects will not directly lead to a DHS acquisition program, as it is envisioned that the trade industry will purchase the technologies, but rather are intended to demonstrate the ability of the technologies to meet DHS's technical requirements.

³The Office of Policy Development is located within DHS's Office of Policy.

⁴DHS, *Developing Operational Requirements: A Guide to the Cost Effective and Efficient Communication of Needs*, Version 2.0 (November 2008).

outlining the performance of the technologies under evaluation to identify the capabilities of the technologies and performance deficiencies. We also reviewed each of the project schedules and compared them to the current status of each of the container security technology projects as of June 2010. We interviewed senior officials in S&T's Borders and Maritime Security Division in Washington, D.C., who are responsible for the four container security projects to discuss the status of the projects. We also interviewed officials representing the four members of the Container Security Test and Evaluation (CSTE) team created by S&T to test and evaluate the technologies—Lawrence Livermore National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories, and the Space and Naval Warfare Systems Center Pacific—to discuss the results of the four projects' test and evaluation processes. In addition to these interviews, we also conducted a site visit to Sandia National Laboratories in Albuquerque, New Mexico—the location for all laboratory testing of the container security technologies—to view technology prototypes, observe the test facilities, and to learn more about the specific laboratory tests that have been conducted on the container security technologies. We also met with officials representing the vendors whose technologies were under testing and evaluation at the time our audit began in October 2009—Georgia Tech Research Institute (GTRI); iControl, Inc.; Maine Secure Composites (MSC); and Science Applications International Corporation (SAIC)—to discuss how they have developed and modified their technologies. Further, we reviewed the contracts and interagency agreements that provided funds to the CSTE team and vendors to determine the amount of money DHS has spent on testing, evaluating, and developing the technologies since funding for the container security technologies began, in April 2004, through 2009.

To address the second objective, we discussed container security technology implementation plans with officials from DHS's Office of Policy Development Transportation, Cargo & Infrastructure Unit, and with CBP officials from its Office of Field Operations and its Customs-Trade Partnership Against Terrorism (C-TPAT) Office.⁵ We also spoke with Department of Defense (DOD) entities, including the U.S. Army and the

⁵Through the C-TPAT program, CBP develops voluntary partnerships with members of the international trade community comprised of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies agree to improve the security of their supply chains in return for various benefits, such as reduced examination of their cargo. See [GAO-08-240](#) for our previous work reviewing the C-TPAT program.

U.S. Transportation Command, to identify any lessons learned from DOD's implementation of container security devices in transporting supplies and equipment to support war efforts in Afghanistan. With representatives of the International Organization for Standardization (ISO)⁶ and World Customs Organization (WCO),⁷ we discussed the process for obtaining international adoption of container security technology standards, and the imposition of duties and taxes on container security technologies, respectively. Further, we spoke with trade industry representatives to understand the trade industry's perspective on how container security technologies could be implemented in the global supply chain, and to identify any potential challenges to implementation. Specifically, we spoke with officials from the World Shipping Council, which represents vessel carriers that transport cargo containers, as well as with two individual vessel carriers and one non-vessel operating common carrier.⁸ We also spoke with representatives from two trade industry associations—the American Association of Exporters and Importers and the National Association of Manufacturers—as well as 22 individual U.S. importers the trade association members identified for us among their membership. We conducted interviews with these importers in group settings. This interview format allowed us to determine consensus and also identify and examine instances where viewpoints differed among importers. As a result of the group settings, we do not explicitly identify the number of importers who expressed particular views. Rather, we express these views as those of some of the importers we interviewed. Further, we met with an official from the Institute of International Container Lessors, which represents companies that lease containers to members of the trade industry, including vessel carriers and importers. Our interviews with these trade industry representatives were based on a nonprobability sample, so they are not generalizable to the entire maritime trade industry, but they did provide us with insights into the willingness of members of the maritime trade industry to partner with DHS and CBP to implement container security technologies, and identify potential challenges to implementation.

⁶ISO is a nongovernmental organization that develops and publishes international standards for which there is a market requirement. ISO standards are voluntary, as ISO has no authority to enforce the implementation of its standards.

⁷The WCO is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of customs administrations.

⁸A non-vessel operating common carrier buys space aboard a vessel and then sells the space to small shippers.

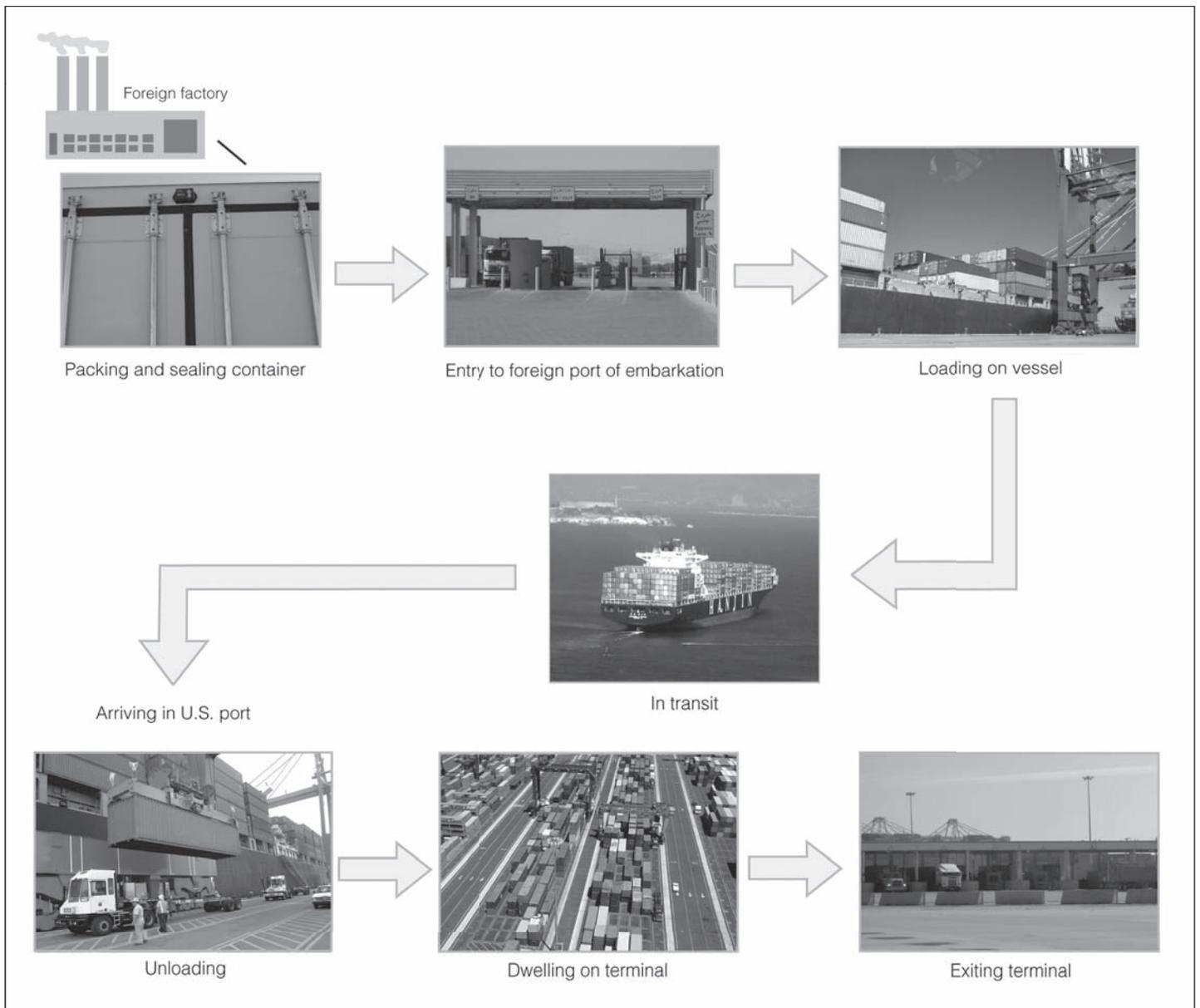
We conducted this performance audit from October 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Global Supply Chain

Given the complexity of the supply chain and the vast number of cargo containers that are shipped to the United States, the supply chain is vulnerable to threats. The typical supply chain process for transporting cargo containers to the United States involves many steps and participants. The cargo container, and material in it, can be affected not only by the manufacturer or supplier of the material being shipped, but also by vessel carriers who are responsible for transporting the material to a port, as well as by personnel who load and unload cargo containers onto vessels. Others who may 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 a vessel. Figure 1 depicts the key participants and points of transfer involved in the supply chain—from the time that a container is packed with cargo in a foreign location to its arrival at a U.S. port.

Figure 1: The Maritime Supply Chain Process



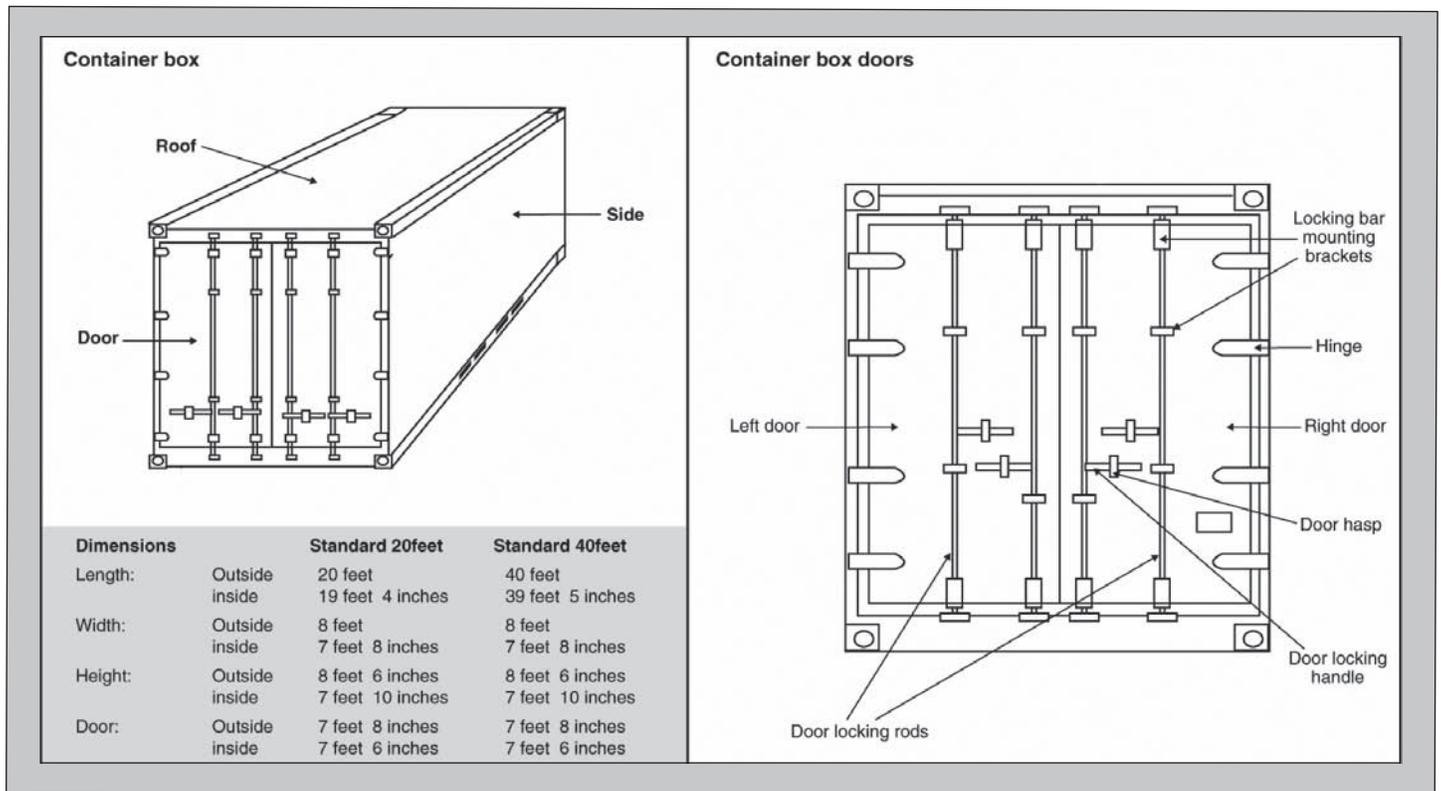
Source: GAO (analysis); GAO and DHS S&T (photos).

Containers serve, in essence, as packing crates and portable warehouses for virtually every type of general cargo moving in the supply chain. The

ISO recommends the standard size of containers. The recommended lengths for cargo containers, according to ISO, are 10 feet, 20 feet, 30 feet, and 40 feet. However, the most common containers are the 20-foot and the 40-foot models.⁹ Container sizes are standardized so that containers can be stacked, and so that loading and unloading equipment can be designed to those standards. Figure 2 shows a typical cargo container and parts of the container door, and summarizes the standard dimensions of 20-foot and 40-foot containers. The basic parts of a typical cargo container are the floor, roof, sides and doors. The floor may be hard or soft laminated wood, planks, or plywood. Modern steel containers have corrugated or flat steel sheet roofs welded to the frame. The sides of steel containers have corrugated steel panels. The hinged doors have plastic- or rubber-lined door gaskets as seals to protect against moisture.

⁹The standard measure of the volume of containerized cargo is a twenty-foot equivalent unit (TEU). For example, one 40-foot cargo container, the most common size in U.S. trade, would be counted as 2 TEUs of cargo.

Figure 2: Drawings of a Typical Cargo Container, Its Parts, and Dimensions



Source: GAO.

CBP Has Developed a Layered Strategy to Secure Cargo Containers

CBP has developed a layered security strategy to mitigate the risk of an attack using cargo containers. CBP's strategy is based on a layered approach of related programs that attempt to focus resources on potentially risky cargo shipped in containers while allowing other cargo containers to proceed without unduly disrupting commerce into the United States. The strategy is based on obtaining advanced cargo information to identify high-risk containers, utilizing technology to inspect containers, and partnering with foreign governments and the trade industry. A brief description of the core programs that comprise CBP's layered security strategy for cargo containers is provided in table 1.

Table 1: Description of CBP's Core Cargo Security Programs

Program and year introduced	Description
Obtaining advanced information to identify high-risk containers	
Automated Targeting System (ATS), 1999	CBP uses ATS—a mathematical model that uses weighted rules to assign a risk score to arriving cargo shipments based on shipping information—to help identify and prevent potential terrorists and terrorist weapons from entering the United States. ATS is used by CBP to review documentation, including cargo manifest information ^a submitted by the vessel carriers on all U.S.-bound 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	CBP generally requires vessel carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before U.S.-bound cargo is loaded onto a vessel at a foreign port. The information is used by ATS in its calculation of risk scores. The cargo manifest information is submitted by vessel carriers for all arriving cargo shipments.
Importer Security Filing and Additional Carrier Requirements (also known as 10+2), 2009	CBP requires importers and vessel carriers to provide data elements for improved identification of containers that may pose a risk for terrorism. The importer is responsible for supplying CBP with 10 shipping data elements, such as country of origin, 24 hours prior to loading, while the vessel carrier is required to provide 2 data elements, container status messages and stow plans, not required by the 24-hour Rule.
Domestic scanning technology deployments	
Non-intrusive inspection (NII) equipment, 2001	CBP uses NII equipment to actively scan both randomly selected containers and those identified by ATS as high-risk. NII uses X-rays or gamma rays to scan a container and create images of the container's contents without opening it. According to CBP, as of August 2010, it had deployed 92 NII systems to U.S. seaports to scan containers. In fiscal year 2009, 4.6 percent of containers arriving at U.S. seaports were scanned.
Radiation Portal Monitors, 2007	CBP program to passively scan 100 percent of containers arriving in the United States with radiation detection equipment prior to leaving a domestic port. According to CBP, as of August 2010, it had deployed 453 radiation portal monitors at U.S. seaports, through which approximately 99 percent of all containers arriving by sea passed.
Partnerships with foreign governments	
Container Security Initiative (CSI), 2002	CBP places staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that their foreign counterparts examine the contents of the containers.
Secure Freight Initiative (SFI), 2006	CBP and Department of Energy program at selected ports to actively and passively scan 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas using integrated examination systems that couple NII and radiation detection equipment.
Partnership with trade industry	
Customs-Trade Partnership Against Terrorism (C-TPAT), 2001	CBP develops voluntary partnerships with members of the international trade community comprised of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies agree to improve the security of their supply chains in return for various benefits, such as a reduced examination of their cargo.

Source: GAO summary of information provided by DHS.

^aCargo manifests are prepared by the vessel carrier for each shipment of cargo loaded on a vessel to describe the contents of the shipment.

Legislation Enacted to Improve Cargo Container Security

Several U.S. laws and regulations govern the security of cargo containers and the supply chain within which they are transported. In 2006, Congress passed, and the President signed, the Security and Accountability for Every (SAFE) Port Act.¹⁰ The SAFE Port Act established a statutory framework for some of the programs comprising CBP's layered security strategy, including CSI and C-TPAT, which previously had been agency programs not required by law. The SAFE Port Act also required that DHS initiate a rulemaking process and subsequently issue an interim final rule to establish minimum standards and procedures for securing containers in transit to the United States. In August 2007, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) was enacted, amending this SAFE Port Act requirement.¹¹ Specifically, the 9/11 Act required that if the interim final rule was not issued by April 1, 2008, then effective no later than October 15, 2008, all containers in transit to the United States would be required to use an ISO 17712 compliant seal.¹² DHS did not establish standards by the set deadline, so all maritime containers in transit to the United States are now required to be sealed with an ISO 17712 compliant seal. According to DHS, it did not establish minimum standards for securing cargo containers in transit because there were no available technology solutions at the time that would adequately improve container security without significantly disrupting the flow of commerce. Although the 9/11 Act default standard is now in effect, the act provides that this standard will cease to be effective upon the effective date of a rule issued in the future pursuant to the original SAFE Port Act requirement.

In addition to the possibility of a future rulemaking in this area, DHS remains responsible for implementing an earlier provision enacted by the Maritime Transportation Security Act of 2002 (MTSA).¹³ This provision requires DHS to establish a program to evaluate and certify secure systems of international, intermodal transportation. This program is to include standards and procedures for securing cargo and monitoring security

¹⁰Pub. L. No. 109-347, 120 Stat. 1884.

¹¹Pub. L. No. 110-53, § 1701(b), 121 Stat. 266, 491 (amending 6 U.S.C. § 944(a)(4)).

¹²Generally, ISO 17712 requires that container seals meet or exceed standards for strength and durability so as to prevent accidental breakage, early deterioration (due to weather conditions, chemical action, etc.) or undetectable tampering under normal usage. ISO 17712 also requires that each seal be clearly and legibly marked with a unique identification number.

¹³46 U.S.C. § 70116.

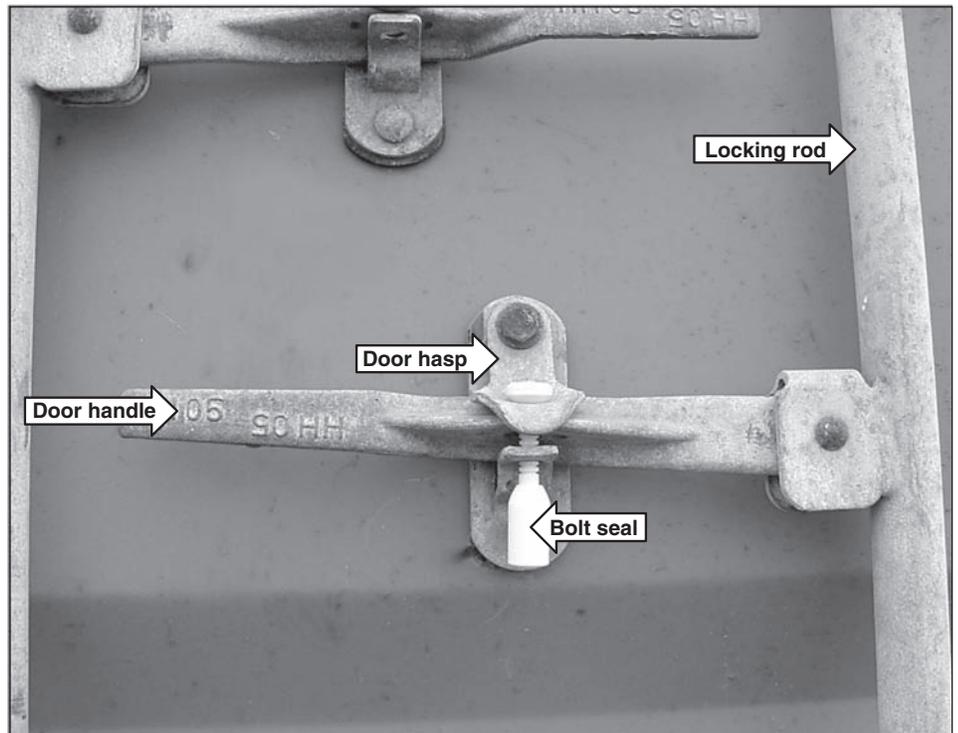
while in transit, as well as performance standards to enhance the physical security of shipping containers, including standards for seals and locks. This provision continues to govern DHS efforts to establish standards for new technology in the cargo container security area.

**Past CBP Efforts Identified
Need for Container
Security Technologies**

In response to a July 2002 memo from the then-CBP Commissioner, CBP undertook a study to identify and evaluate available technologies to improve container security. The study demonstrated that existing container seals provided inadequate security against physical intrusions. We reported in January 2006 that despite the widespread use of container seals, they are not effective in preventing tampering.¹⁴ For example, entry into a container through the roof or sides will not be indicated by a container seal affixed to the doors. Further, various methods to circumvent seals installed on container door hasps (see fig. 3) have been demonstrated by the Department of Defense and the Vulnerability Assessment Team at Los Alamos National Laboratory. Seals installed through the door hasp can be bypassed and left intact by simply removing an entire container door. Recognizing the limitations of existing container technology, CBP desired a technology with the ability to monitor and record door openings and eventually detect and report intrusions on all six sides of a container. Figure 3 shows a container with a bolt seal affixed to the door hasp.

¹⁴This report is restricted and not available to the public.

Figure 3: A Container Sealed with a Bolt Seal



Source: CBP (photo), GAO (presentation).

CBP initiated the Smart Box program in 2004 in order to develop technologies with the ability to monitor the physical integrity of a container, among other things. In September 2005, CBP, in consultation with Johns Hopkins University Applied Physics Laboratory, determined through operational testing that there was no existing container security device that could meet its requirements. CBP made a second attempt, in December 2007, to find a commercially available container security device with the ability to monitor container doors for intrusion. According to CBP officials, only one security device—offered by General Electric—demonstrated the potential to meet CBP’s requirements. However, according to CBP, subsequent operational testing revealed that the device had a relatively high false alarm rate, which, according to CBP officials, would have resulted in an unmanageable workload for CBP staff at ports given the number of containers they would have to examine because of the alarms. According to CBP officials, before they could schedule another round of testing to determine if a revised prototype of the device would

meet CBP's requirements, General Electric decided to stop producing the device.

DHS S&T Initiated Four Projects to Develop Container Security Technologies

S&T is developing four container security technologies, which are described in table 2, in response to MTSA requirements and CBP's need for container security technologies with the ability to detect intrusion and track the movement of containers through the supply chain. In May 2004, S&T issued a broad agency announcement for the Advanced Container Security Device (ACSD) project seeking industry submissions for technologies that could be developed to provide six-sided intrusion detection for cargo containers. The initial results of ACSD testing demonstrated that a solution would require years of additional investment and development. As a result of the challenges, DHS created the Hybrid Composite Container to embed six-sided detection in a container made of composite material, and the Container Security Device (CSD) project to provide the capability to detect container door intrusion as an interim solution until six-sided detection is available. In November 2003, S&T issued a small business innovative research (SBIR)¹⁵ solicitation seeking a Marine Asset Tag Tracking System (MATTS) with the capability to provide both worldwide container tracking, and communicate the security status of the CSD and ACSD in the supply chain. Table 2 provides a description of each of the four container security technology projects, including the projects' goals, key vendors, and time frames.

¹⁵The goal of a small business innovative research (SBIR) program is to incentivize increased participation of innovative and creative small businesses in federal research / federal research and development programs and to challenge industry to bring innovative homeland security solutions to reality.

Table 2: Description of DHS S&T’s Four Container Security Technology Projects

Project name	Project description and goal	Key vendors ^a	Project start ^b	Project completion ^c
Advanced Container Security Device	Develop a device that can detect and report container intrusion on all six sides of a container.	<ul style="list-style-type: none"> L-3 Communications SAIC 	2005	2012
Container Security Device	Develop a device that can detect and report the opening and removal of container doors.	<ul style="list-style-type: none"> GTRI SAIC 	2007	2011
Hybrid Composite Container	Develop an ISO certified container using a steel frame and fiber reinforced polymer composite material for the walls, floor, and doors, with embedded security sensors to detect intrusion on all six sides of a container.	<ul style="list-style-type: none"> Maine Secure Composites (container) GTRI (sensor grid) 	2005	2012
Marine Asset Tag Tracking System	Establish a system to track containers, and increase the range that CSD and ACSD status information can be transmitted.	<ul style="list-style-type: none"> iControl, Inc. 	2004	2010

Source: GAO analysis of DHS S&T information.

^aKey vendors are those selected in the most recent round of vendor selection for each project. App. I provides additional details on the vendor selection process.

^bThe project start date is the fiscal year in which a vendor award was first made.

^cThe project completion date is the anticipated fiscal year in which the performance standards are to be provided to the Office of Policy Development and CBP, as stated in S&T’s *Five-Year Research and Development Plan: Fiscal Years 2008-2013*.

S&T’s overall objective for each of these container security technology projects is the development and delivery of performance standards for the technologies to DHS’s Office of Policy Development and CBP.

Performance standards define a set of requirements that must be met by products to ensure they will function as intended. Before S&T can provide performance standards to the Office of Policy Development and CBP, the capability of the technologies to meet stated requirements must be demonstrated through the successful completion of testing and evaluation activities, as described in the technology transition agreements.¹⁶ S&T has defined two phases of testing and evaluation for these projects:

- **Phase I—Laboratory Testing:** The purpose of Phase I is to identify capabilities and deficiencies in prototypes in a controlled environment

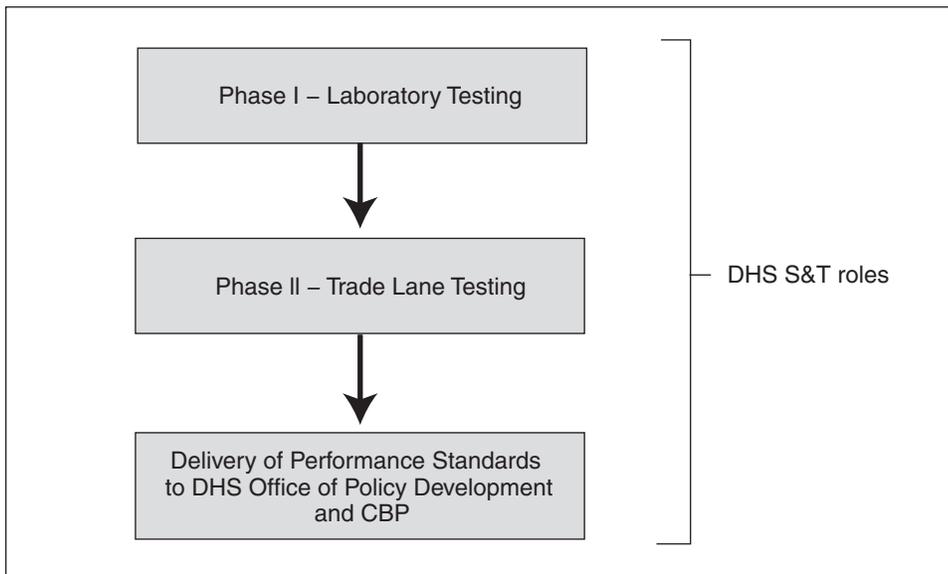
¹⁶Technology transition agreements are agreements signed by S&T and its customers that describe the capability gap that the S&T project will fill, the project deliverable, the technical requirements and parameters, and the project plan.

to determine the likelihood of a prototype functioning under a variety of anticipated environmental and usage conditions. At least 10 prototypes are used for Phase I testing of a technology.

- **Phase II—Trade Lane Testing:** Phase II is designed to determine whether a prototype can enhance supply chain security while minimizing the effect on cargo operations. Phase II includes testing in an operational trade lane—the route a container travels—using 100 trips from the container packing location to arrival at a U.S. port.

After successful completion of both phases of testing, S&T is to deliver performance standards—including system requirements and test plans—to the Office of Policy Development and CBP. Figure 4 shows how the testing process leads to the development of performance standards.

Figure 4: DHS S&T Testing Process



Source: GAO analysis of DHS S&T information.

DHS Has Made Progress in Researching and Developing Container Security Technologies, but Needs to Conduct Testing Using Defined Operational Scenarios before Delivering Performance Standards

From 2004 through 2009, S&T spent over \$60 million and made varying levels of progress in the research and development of its four container security technology projects—ACSD, CSD, Hybrid Composite Container, and MATTS—to support the development of performance standards for these container security projects. Each of these projects has undergone Phase I laboratory testing, but S&T has not yet conducted Phase II trade lane testing in an operational environment to ensure that the prototypes will satisfy the requirements so that S&T can provide performance standards to the Office of Policy Development and CBP. Prior to the development of performance standards by S&T, each of the technology prototypes will need to undergo Phase II trade lane testing consistent with the operational scenarios that have been identified for potential implementation. According to S&T, the master test plans do not reflect all operational scenarios being considered because DHS is currently focused on using the technologies in the maritime environment.

DHS S&T Has Identified and Funded Vendors' Container Security Technologies for Development

S&T used a multiple-round process to select vendors' technologies for development. Several vendors responded to S&T's 2004 broad agency announcement for the ACSD project and 2003 SBIR solicitation for MATTS. The vendors' technology proposals were evaluated on their ability to meet the project requirements, and those technologies considered to be viable were funded by S&T to develop prototypes for test and evaluation. Because of the challenges in developing an ACSD solution, S&T created the CSD project and selected vendors for the project based on the performance of vendors' prototypes during ACSD project testing. Similarly, selection for the Hybrid Composite Container project was based on performance in the ACSD project. From 2004 through 2009, S&T has provided a total of about \$24 million in funding to vendors to develop container security technologies. Appendix I provides additional details on the vendor selection process.

S&T created the Container Security Test and Evaluation (CSTE) team to develop requirements and independently monitor and evaluate the performance of container security technologies. CSTE membership is composed of three Department of Energy national laboratories—Lawrence Livermore National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories—and the Navy's Space and Naval Warfare Systems Center Pacific. As described in table 3, these organizations were each selected for participation based on their areas of applicable technical expertise in fields such as sensor systems, wireless

communications, and maritime environment product testing. From 2004 through 2009, S&T obligated nearly \$36 million to the CSTE team to develop requirements and conduct testing and evaluation of container security technologies.

Table 3: Members of the Container Security Test and Evaluation (CSTE) Team and Their Respective Roles and Responsibilities on the Container Security Technology Projects

CSTE team member	Key responsibility / Field of expertise
Lawrence Livermore National Laboratory	Determine maritime environmental conditions to establish laboratory tests to determine the ability of container security technology prototypes to function in the maritime environment.
Pacific Northwest National Laboratory	Contribute expertise in sensor development, wireless technologies, electronics management, and embedded systems.
Sandia National Laboratories	Perform all container security technology prototype testing at their facilities in New Mexico. Provide red teaming—the capability to identify and exploit weaknesses in a technology—and general systems engineering support.
Space and Naval Warfare Systems Center Pacific	Serve as the contracting office—create vendor contracts, issue work orders, and distribute funding. Develop wireless communications requirements and device readers.

Source: GAO summary of Department of Energy and DOD information.

One of the responsibilities of the CSTE team was to develop test plans that specify the testing activities that technologies need to successfully undergo in order to move on to later phases of testing and eventually the development of performance standards. These test plans require that technologies be evaluated on their installation and usability, functionality, performance (including under adverse environmental conditions), and vulnerability to attack by an adversary.

S&T Has Identified Deficiencies That Could Delay or Prevent the Development of Standards for Some Container Security Technologies

The CSD project is expected to be completed on time, and MATTS is slightly behind schedule, as performance standards are expected to be delivered in December 2010 rather than fiscal year 2010. The ACSD project is not currently being funded due to the deficiencies identified during Phase I laboratory testing, although funding may resume if one of the vendors demonstrates progress. The Hybrid Composite Container project is undergoing contract negotiations to resume work on the composite container after challenges were encountered with the vendor. Table 4 summarizes the status and expected completion date for each of S&T's container security technology projects.

Table 4: Status of Container Security Technology Projects

Project name	Key project requirements	Project status	Expected completion (fiscal year)
Advanced Container Security Device (ACSD)	<ul style="list-style-type: none"> • Detect container door opening, door closing, and door removal. • Detect a 3-inch diameter hole in the container on any six sides. • Detect human presence within the container. • Provide a 95 percent probability of intrusion detection. • Provide a combined probability of false alarm and critical failure of 0.2 percent. • Possess a power source to operate for one trip (1,680 hours). • Cost less than \$175 per container trip. 	<p>Stopped in Phase I laboratory testing. Because of deficiencies in satisfying ACSD requirements during laboratory testing, no ACSD prototypes are currently being funded for development. S&T may resume funding of one vendor's prototype if the vendor demonstrates progress in improving performance of its CSD.</p>	2012
Container Security Device (CSD)	<ul style="list-style-type: none"> • Detect container door opening, door closing, and door removal. • Monitor the status of any seals or locks. • Provide a 95 percent probability of intrusion detection. • Provide a combined probability of false alarm and critical failure of 0.2 percent. • Possess a power source to operate for one trip (1,680 hours). 	<p>Progressing to Phase II trade lane testing. CSDs have shown promise in laboratory testing, and S&T anticipates beginning Phase II trade lane tests for one CSD prototype in September 2010.</p>	2011
Hybrid Composite Container	<p>Composite container</p> <ul style="list-style-type: none"> • Meet or exceed ISO requirements. <p>Sensor grid</p> <ul style="list-style-type: none"> • Detect a 3-inch diameter hole in any six sides of a container. • Provide a 95 percent probability of intrusion detection. • Provide a combined probability of false alarm and critical failure of 0.2 percent. • Possess a power source to operate for one trip (1,680 hours). 	<p>Stopped in Phase I laboratory testing. S&T terminated the contract with the vendor because of internal management issues the vendor was having. S&T plans to initiate a new contract to continue the work before the end of September 2010.</p>	2012

Project name	Key project requirements	Project status	Expected completion (fiscal year)
Marine Asset Tag Tracking System (MATTS)	<ul style="list-style-type: none"> Communicate a container intrusion alarm within 5 minutes of the alarm occurring. Provide operational availability at least 95 percent of the time. Possess a power source to operate for 30,000 hours. Cost less than \$175 per container trip. 	Progressing to Phase II trade lane testing. MATTS is scheduled to participate in Phase II trade lane tests with the CSD in September 2010.	2011

Source: GAO analysis of DHS S&T information.

In order for these container security technologies to provide the functionality that DHS desires, they must interface with readers—both handheld and fixed in place—that can use wireless communications to send commands to or gather operational or intrusion alarm status information from the technologies for CBP’s use. Readers also serve as a means to arm and disarm ACSDs (including the sensor grid embedded in the Hybrid Composite Container) and CSDs. Because ACSDs and CSDs are mounted on the interior of a container in a manner that protects them from being physically accessed from outside of a container, a remote, wireless device such as a reader is needed to turn on the devices’ intrusion detection functionality upon sealing the container (arming the device) and to turn off the devices’ intrusion detection functionality when the container is opened by authorized parties (disarming the device). A handheld reader would also allow an official in close proximity to the container to detect and read the ACSD or CSD to determine if the container had been opened after it was sealed. In contrast, a fixed reader has a longer range and would be designed to automatically relay such status information to a centralized data center. ACSDs and CSDs must also support an encryption scheme for two reasons. First, commands to disarm a device must be encrypted to prevent unauthorized parties from circumventing the device by disarming it. Second, status information that a device sends may contain sensitive information, so status messages must be encrypted to protect the information during wireless transmission. Devices, such as handheld readers, would then be “trusted,” in that they would have the ability to handle encrypted communications with ACSDs and CSDs. Appendix II provides further information on the planned communications system supporting ACSDs and CSDs.

S&T Halted ACSD Funding during Phase I Laboratory Testing Because of Performance Deficiencies

According to S&T, because of deficiencies observed in Phase I laboratory testing, it is not currently funding the development of any vendor’s ACSD prototype beyond Phase I laboratory testing. S&T officials added that L-3 Communications (L-3) and SAIC, the two vendors selected to participate in Phase I laboratory testing, did not demonstrate enough progress meeting the requirements. According to S&T and CSTE team officials, meeting the requirements of the ACSD program, including detecting intrusion on all six sides of a container, has proven to be very challenging. According to S&T, it may resume funding for the development of the SAIC ACSD if SAIC demonstrates sufficient improvement in its CSD, which uses similar technology. If no ACSD is found to demonstrate enough progress in meeting the requirements, performance standards will not be delivered for this project. Table 5 summarizes the test results for the ACSDs.

Table 5: Description of CSTE’s Testing of the ACSD Prototypes

Vendor	Testing status	Test summary
L-3 ^a	Phase I laboratory testing was conducted from April to September 2008, and resulted in the CSTE team recommendation that no further testing be conducted.	<ul style="list-style-type: none"> • Installation was difficult and could potentially injure the installing personnel. • Device confounded by environmental noise. • Detected 10 percent of wall penetration events, but near 0 percent when the container was loaded with cargo near the device. • Detected 96 percent of door openings. • No specific environmental testing, but observed to possibly be vulnerable to damage from dropping and condensation.
SAIC ^b	Phase I laboratory testing was conducted from April to June 2008, and resulted in the CSTE team recommendation that no further testing be conducted. Testing may resume if progress is made on SAIC’s CSD.	<ul style="list-style-type: none"> • Installation was reasonable and safe, but includes a complicated calibration step. • Operation was inconsistent and unpredictable. • It could not reliably detect a 3-inch diameter hole in the container, but could more easily detect when an object is inserted into or removed from the container through such a hole. • Extensive false alarms occurred, so no specific environmental testing was done.

Source: GAO analysis of DHS S&T information.

^aThe L-3 ACSD is a large, 50-pound device that is to be mounted inside the container, above the door, and run the full width of the interior of the container. It relies on a suite of light, acoustic, carbon dioxide, and other sensors to detect intrusion and human presence inside a container.

^bThe SAIC ACSD consists of a single unit mounted inside the container, over the door. It uses radio frequency resonance to detect intrusion attempts. The device emits radio frequency signals and monitors the characteristics of the reflected signal to infer any changes in the structure of the container. Changes in the radio frequency reflections may indicate an opening in the container. This technique may not be as effective on Hybrid Composite Containers.

During Phase I laboratory testing, conducted from April 2008 to September 2008, the L-3 ACSD prototype successfully detected container door openings. However, it failed to identify preexisting holes in containers, was unable to consistently detect wall intrusions in ideal (empty container) conditions, and was largely unable to detect wall intrusions in a

loaded container. Consequently, the L-3 ACSD prototype failed the project requirement that a device detect a hole in a container. According to S&T, based on the conclusions of the CSTE Team, in October 2008, S&T decided not to fund the L-3 ACSD for additional testing and evaluation.

During Phase I laboratory testing, conducted from April 2008 to June 2008, the SAIC ACSD prototype detected door openings and closings, but it generated a false alarm rate higher than that permitted by the ACSD project requirements. Similar to the L-3 ACSD, in September 2008, the CSTE team concluded the SAIC ACSD was deficient. S&T decided that no further funding be provided to SAIC for the ACSD project. However, according to S&T officials, SAIC's ACSD prototype is closely related to that of its CSD (see below), and therefore, if SAIC's CSD demonstrates improvement, S&T will consider funding SAIC's ACSD for further tests and evaluations.

CSD Performance Has Varied and S&T Anticipates One Vendor's CSD Prototype Will Begin Phase II Trade Lane Testing

Performance of the two CSD prototypes varied during Phase I laboratory testing and, according to the S&T program manager, Phase II trade lane testing is expected to begin for one of the prototypes in late 2010. S&T anticipates that Phase II trade lane testing will begin for the GTRI CSD in September 2010. According to S&T officials, the SAIC CSD began another round of Phase I laboratory testing in May 2010, but testing has since ceased due to the high false alarm rate the device exhibited. The S&T program manager expects to meet a November 1, 2010, due date for completion of CSD performance standards for the Office of Policy Development and CBP. Table 6 summarizes the test results for the CSDs.

Table 6: Description of CSTE’s Testing of the CSD Prototypes

Vendor	Testing status	Test summary
GTRI ^a	Phase I laboratory testing was conducted in 2007, and another round in 2009. A new version addressing the identified deficiencies was delivered to DHS in 2010. Phase II trade lane tests are anticipated to begin in September 2010.	<ul style="list-style-type: none"> • Installation was reasonable. • Detected 100 percent of door openings during valid tests. • CSTE noted false alarms or failures, or both, during temperature shock, humidity, and vibration tests. • Communications system required improved reliability and consistency. • Vulnerability testing revealed some weaknesses, such as a lack of built-in tamper resistance.
SAIC ^b	Phase I laboratory testing was conducted from April to November 2008. A new version addressing the identified deficiencies was delivered to DHS in May 2010 and is being evaluated by the CSTE.	<ul style="list-style-type: none"> • Installation was reasonable and safe, but includes a complicated calibration step. • Detected 98 percent of door openings in empty containers and 96 percent in loaded containers. • False alarm rates ranging from 0 to 100 percent occurred when the test team shifted the location of cargo in the container. • False alarms occurred during container stacking tests and during humidity, saltwater mist, static discharge, and vibration tests.

Source: GAO analysis of DHS S&T information.

^aThe GTRI CSD consists of three components—two door-mounted units, and a header-beam-mounted controller unit. The GTRI CSD uses light-emitting diodes and light sensors to measure the position of the container doors. The infrared light-emitting diodes in each of the two door units emit light pulses, which the controller unit authenticates as having come from a CSD door unit. The device alarms when it detects a door opening of 1 inch or greater, or a decrease in signal strength past a set threshold.

^bThe SAIC CSD is identical in appearance and general function to the company’s ACSD. The primary difference between the two devices is in the sensing algorithm. The ACSD attempts to monitor all six sides of the container, whereas the CSD is focused on detecting the opening or removal of the container doors.

While the GTRI CSD reliably and consistently detected container door openings, minor deficiencies in environmental durability and physical security were identified in the first set of Phase I laboratory testing. GTRI responded to the identified deficiencies and submitted a revised prototype for additional Phase I laboratory testing. According to the S&T program manager, S&T determined that GTRI appropriately modified its prototype to resolve the deficiencies identified in the last round of Phase I laboratory testing, and S&T plans to include this device in Phase II trade lane testing scheduled to begin in September 2010. The S&T program manager added that during Phase II trade lane testing, the CSD will be installed on containers that will travel from the Port of Shanghai, China, to Savannah, Georgia. Figure 5 shows photographs of GTRI’s and SAIC’s CSDs, which are mounted on the interior of cargo containers.

Figure 5: Photographs of GTRI's and SAIC's Container Security Devices



Source: DHS.

The SAIC CSD reliably and consistently detected door openings, but frequent false alarms, deficiencies in the connections of electrical components, and deficiencies in the device's installation and mounting system were identified during Phase I laboratory testing. According to SAIC, it is adjusting the detection algorithms, which is expected to reduce the device's sensitivity to normal cargo shifting during transit in an effort to reduce the device's false alarm rate, and it expects to simplify the installation procedure to address S&T's concerns. According to the S&T program manager, the new version of SAIC's CSD was delivered to S&T in May 2010 and during Phase I testing and evaluation it exhibited a high false alarm rate.

The Hybrid Composite Container Project Has Demonstrated Potential, but S&T Terminated the Vendor's Contract during Phase I Laboratory Testing Because of Internal Management Issues

According to S&T, it terminated MSC's contract to build the composite container for the Hybrid Composite Container Project in June 2010 because MSC was experiencing internal management issues that were preventing the project from progressing. MSC had been building an ISO-compliant 20-foot shipping container made out of a composite fiber material instead of steel. The container consists of 4-foot by 8-foot corrugated, fiber-reinforced polymer panels welded to a steel frame. Five of the panels are welded together to form a 20-foot container wall. The container is 15 percent lighter than a steel container of the same size, and according to an official at the University of Maine (a subcontractor to MSC), it is expected to exhibit three to five times greater resistance to corrosion than a steel container. Damaged panels must be replaced, however, rather than repaired with a patch as can be done on a steel

container. The container incorporates an embedded sensor grid to provide six-sided intrusion detection. In addition to the sensor grid, the composite container is to use a CSD for door-opening detection. Finally, a communications chip is integrated into the sensor grid to allow for wireless communications with readers.

Previous test results of the composite container indicate that the container would likely meet or exceed ISO standards and, therefore, be suitable for use in international trade. S&T selected GTRI to develop a sensor grid that could be embedded within the walls of the composite container to provide intrusion detection capability. The sensor grid provides ACSD-like security for the container in that a hole in the container wall would be detected by the sensor grid triggering an alarm. However, one of the composite panels with the embedded sensor grid failed durability testing conducted by the vendor. Although development of the composite container has been halted, S&T has directed GTRI to continue developing its sensor grid to address this deficiency because S&T is exploring other contracting options to continue the development of the composite container. According to S&T, it anticipates that work on the composite container will resume in September 2010.

Marine Asset Tag Tracking System Is Progressing to Phase II Trade Lane Testing

One vendor, iControl, Inc., is currently being supported by S&T to develop MATTS, which includes the iTAG, a communications tag mounted on the exterior of containers, and the iGATE, a remote reader used to communicate with the iTAG. MATTS will participate in Phase II trade lane testing with the GTRI CSD in September 2010. MATTS provides the capability to globally track the location of containers. In addition, the MATTS iTag provides a long-range wireless communications system for CSD and ACSD devices.¹⁷ A CSD or ACSD device mounted on the interior of a container has a short-range wireless communications system, but the iTAG, when mounted outside of a container, can act as a relay to pass messages from the CSD or ACSD to centralized locations at a designated read point, such as a port of departure.¹⁸ The CSTE team conducted limited Phase I laboratory testing of the iTAG, but it did not conduct all needed laboratory testing because changes were still being made to the

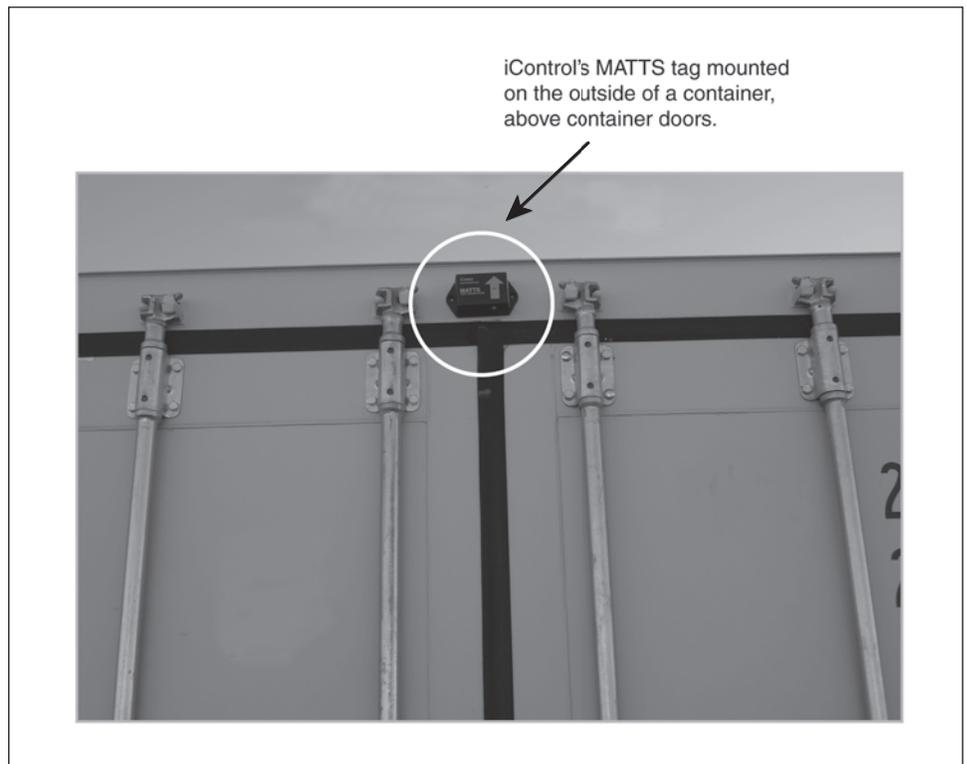
¹⁷During testing, the performance of the iTAG's long-range communications system varied from 341 meters to 3,699 meters.

¹⁸ACSDs and CSDs are required to communicate with handheld readers within 10 feet and fixed readers within 100 feet.

iTAG. According to the S&T program manager, the iTAG will undergo all required testing when it is produced in its final form.

While MATTS has not undergone DHS's Phase II trade lane tests, iControl, Inc., conducted two trade lane tests of MATTS beginning in 2007 and 2008. During each of these trade lane tests, iControl, Inc., placed 100 iTAGs on 100 cargo containers and shipped them from the Port of Yokohama, Japan, to the Port of Los Angeles. At the conclusion of these tests, 199 of the 200 MATTS iTAGs arrived at their destinations. However, the trade lane testing identified deficiencies with iControl, Inc.'s MATTS iTAG. Specifically, 13 to 15 percent of the iTAGs sustained damage during the tests, including loose connectors that affected the performance of the MATTS tags. In one test, power management features did not function as intended, resulting in battery usage in excess of that allowed by the project requirements. During the trade lane tests, iControl, Inc., did not test MATTS in conjunction with any ACSD or CSD prototypes. However, iControl, Inc., did test the environmental durability of the iTAG, as well as its power management and container tracking capabilities. According to the S&T program manager, the deficiencies identified in MATTS are being addressed by iControl, Inc., and a new version of the iTAG, in conjunction with the GTRI CSD device, will undergo Phase II trade lane testing from the Port of Shanghai, China, to Savannah, Georgia, in September 2010. The S&T program manager anticipates providing MATTS performance standards to the Office of Policy Development and CBP in December 2010. Figure 6 shows the MATTS tag mounted on a cargo container.

Figure 6: Photograph of iControl, Inc.'s MATTS Tag



Source: DHS.

Testing All Operational Scenarios Would Enable S&T to Better Determine the Performance of Container Security Technologies in Their Intended Operational Environments

Before S&T can provide container security technology performance standards to the Office of Policy Development and CBP, all technology prototypes have to undergo Phase II trade lane testing, according to the master test plans. According to S&T, the MATTS tag and GTRI's CSD are expected to undergo Phase II trade lane testing in September 2010. However, S&T's plans for conducting Phase II trade lane testing of these container security technologies do not reflect all the operational scenarios agreed upon within DHS for how the technologies could be implemented. S&T's master test plans define Phase II trade lane testing as 100 maritime moves to a U.S. port. However, some of the operational scenarios being considered for implementation by the Office of Policy Development and CBP involve using technologies on cargo containers that would either not be placed on a vessel, or only applied during overland shipping after their

arrival in the United States.¹⁹ Before S&T can provide performance standards, per the technology transition agreements signed by S&T, the Office of Policy Development, and CBP, the technologies are to have been proven to work in their final form and under expected operational conditions. DHS acknowledged that the testing is limited and that future testing should reflect all the operational scenarios. Unless the container security technologies are tested in all operational scenarios, the performance standards that are delivered by S&T to the Office of Policy Development and CBP may not fully meet DHS's or CBP's needs. Our prior work has shown that when operational requirements are not established prior to acquisition, it can negatively affect program performance.²⁰ Conducting Phase II trade lane testing for the container security technologies consistent with all operational scenarios would better position S&T to determine if the technologies will be suitable for use in their intended operational environments.

Key Steps and Challenges Remain before Implementation of Container Security Technologies Can Move Forward

If S&T determines that the container security technologies are mature enough to provide performance standards for these technologies to the Office of Policy Development and CBP, key steps and associated challenges remain before DHS and CBP can implement the container security technologies in the supply chain that meet those performance standards. Based on our discussions with Office of Policy Development and CBP officials, we identified three key steps that remain before implementation can occur: (1) obtaining support from trade industry and international partners, (2) developing a concept of operations (CONOPS)²¹ that describes how the technologies are to be deployed, and (3) certifying the technologies for use in the supply chain. According to Office of Policy Development and CBP officials, they will take these steps if and when S&T

¹⁹Three of the four operational scenarios consist of affixing container security devices on containers after their arrival by vessel or for overland shipping and include: (1) C-TPAT members' containers transiting from Mexico to the United States by truck; (2) containers arriving at the Port of Los Angeles and transiting by truck to Texas for immediate export into Mexico; and (3) containers transiting by truck from Mexico to Canada carrying agricultural products potentially containing pests.

²⁰GAO, *Department of Homeland Security: Assessments of Selected Complex Acquisitions*, [GAO-10-588SP](#) (Washington, D.C.: June 30, 2010); and *Defense Acquisitions: DOD Must Prioritize Its Weapon System Acquisitions and Balance Them with Available Resources*, [GAO-09-501T](#) (Washington, D.C.: Mar. 25, 2009).

²¹A CONOPS is a user-oriented document that describes how an asset, system, or capability will be employed and supported from the users' viewpoint.

is able to provide performance standards. Our work indicates that the Office of Policy Development and CBP could face challenges when executing some of these steps.

Obtaining Trade Industry and International Partners' Support to Implement Container Security Technologies Could Be Challenging

DHS could face challenges in obtaining support from the trade industry and international partners as it pursues implementation of the container security technologies. According to an Office of Policy Development director, there are two approaches DHS could likely pursue to implement container security technologies—mandatory or voluntary participation by the trade industry. The director added that if DHS determines that the universal use of container technologies would provide a worthwhile security benefit, DHS would likely pursue a rulemaking approach to mandate the use of the technologies on all U.S.-bound containers. If DHS determines that the technologies would be primarily beneficial in a more limited portion of the supply chain, though, it would work with the trade industry to encourage voluntary use of the technologies. Some members of the trade industry we spoke with were resistant to purchasing and using the technologies given the number of container security programs they already have to comply with.²² Representatives of the World Shipping Council and both vessel carriers we spoke with questioned the role of vessel carriers in implementation because of the uncertainties that presently exist concerning how the technologies could be implemented and which parties are to be involved. The representatives of the two vessel carriers we spoke with expressed interest in purchasing the Hybrid Composite Container because of the commercial benefit that could be provided by its reduced weight, but they added that they are not interested in spending additional money on the embedded sensor grid that is to provide the security benefit. Further, the importers we spoke with questioned their role and whether they have the authority to affix technologies on containers they do not own, as the containers they use are typically leased.

If CBP adopts a voluntary approach, it may also have challenges getting support from C-TPAT members—its trusted private sector partners. Container security technologies could provide security benefits in the supply chain, but using technology that detects intrusion into a cargo

²²As noted earlier, we conducted interviews with importers in group settings. As a result of the group settings, we do not explicitly identify the number of importers who expressed particular views. Rather, we express these views as those of some of the importers we interviewed.

container when there is no assurance illicit materials or contraband were not earlier introduced could give the false impression that the container is secure or could have the effect of potentially locking dangerous or illicit cargo in a container. Since C-TPAT members are committed to a comprehensive security process, including procedures for securing containers at the point of packing, they provide such assurance. According to DHS's 2007 *Strategy to Enhance International Supply Chain Security*,²³ the department intended to use C-TPAT Tier III²⁴ members to implement commercially available container security devices that CBP previously tested. However, C-TPAT Tier III members we spoke with were resistant to the idea of having to purchase and use technologies, such as the CSD and ACSD, on their containers to maintain their Tier III status. In particular, some of the members stated that from a financial standpoint, the additional benefit of reduced number of container inspections that CBP provided to Tier III members over Tier II²⁵ members, would not outweigh the costs of using the technologies. As a result, they stated that they would likely downgrade to Tier II status rather than have to purchase the technologies. The C-TPAT Tier III members, as well as other trade industry representatives we spoke with, said DHS should demonstrate, through a risk-benefit analysis, that using the technologies would provide a clear security benefit before making the use of such technologies a requirement. CBP officials told us that they are aware that the trade industry is generally not willing to spend money on container security technologies and that C-TPAT members question whether the cost is worth the benefit.

In addition to obtaining trade industry support, DHS will also need to obtain support from international organizations and WCO to implement the new container security technologies. In order for the container security technologies to be admitted into foreign countries without being subject to import duties and taxes, as well as import prohibitions and restrictions, the technologies first have to be recognized as accessories and equipment of the containers under the Customs Convention on

²³DHS, *Strategy to Enhance International Supply Chain Security* (July 2007).

²⁴Tier III is for those C-TPAT members that exceed minimum security criteria and demonstrate a commitment to the highest levels of supply chain security.

²⁵While Tier II members must meet minimum security requirements set by the C-TPAT program, Tier III membership is achieved by exceeding minimum requirements. In addition, Tier III members are required to maintain a record that is clear of security breaches or incidents.

Containers. The convention essentially provides for the temporary admission and reexportation of containers and their accessories and equipment that meet certain requirements without the imposition of duties or taxes by any customs authority. According to a WCO director, while an individual device attached to a container most likely would be viewed as an accessory to the container, if multiple devices are shipped in bulk for reuse on other containers, the question of how to treat them for import duty purposes would be more difficult. He also noted that, if requested by a member country, WCO could provide an advisory opinion as to whether the technologies should be treated as container accessories and equipment pursuant to the Customs Convention on Containers, but the ultimate decision as to whether to classify the technologies as exempt from import duties and taxes resides with each individual foreign government.

Other options under consideration for how the container security technologies are to be implemented would also require support from foreign governments. CPB officials told us that they are considering implementing the use of container security technologies in high-risk trade lanes—trade routes that have been determined to pose the highest risk of transporting threats to the United States. S&T officials stated that another option would be to use the technologies on cargo containers departing from ports participating in the Container Security Initiative.²⁶ CBP officials recognize that they will need to work with international partners, and plan to do so when S&T provides performance standards.

Developing a Feasible Concept of Operations Could Prove Difficult

The successful implementation of container security technologies depends on the security procedures throughout the supply chain as well as the people engaged in those procedures. These procedures are typically documented in a concept of operations (CONOPS)—a user-oriented document that describes how an asset is to be employed and supported from the users' viewpoint. A CONOPS also describes the operations that must be performed, who must perform them, and where and how the operations will be carried out. DHS and CBP could face challenges developing a feasible CONOPS that addresses the necessary technology infrastructure needs and protocols. Container security technologies require a supporting technology infrastructure, including readers to communicate to customs officials whether a technology has identified an

²⁶Through the Container Security Initiative, CBP places staff at 58 participating foreign ports through which 86 percent of U.S.-bound cargo containers pass, to work with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States. See [GAO-08-187](#).

unauthorized intrusion, and a means to capture and store the data. CBP will be faced with determining who will have access to the container security technologies through readers, where to place these readers, and obtaining permission to install fixed readers at both domestic and foreign ports. Prior work we conducted on container scanning technologies identified challenges in obtaining permission and space from terminal operators at both domestic and foreign ports to install equipment.²⁷ Further, several pilots previously conducted to test the feasibility of using container security technologies have also noted challenges with establishing the reader infrastructure at ports. For example, during Operation Safe Commerce, difficulties were encountered with the installation and maintenance of fixed readers at both foreign and domestic ports.²⁸ Furthermore, several foreign ports did not allow installation of the fixed readers, and problems were also encountered in installing and maintaining power to fixed readers at domestic port facilities. In addition, databases are needed to collect the data obtained by the readers from the container security technologies. Pilots have also demonstrated the challenges with establishing information systems to collect the data provided by the technologies.

Establishing protocols regarding which supply chain participants will be involved in arming and disarming the technologies, reading the status messages generated by the technologies, responding to alarms, and accessing data will also be important. For example, if the CONOPS calls for technologies to first be affixed to a container at the point of packing, it will require the packers to have the ability to first install and arm the technologies. The packing of goods into cargo containers can be handled by a number of different parties, including the shipper (i.e., seller), a third-party consolidator, or the buyer. Regardless of which party is packing the container, these participants have the last visual check of the goods before they are sealed for transport. At any point during the transfer of the container from its packing point to the port of embarkation, foreign customs may need to stop and open a container for inspection. In these instances, it will be important to ensure foreign customs officials have the ability to arm and disarm the technologies so they can open a container

²⁷GAO-10-12.

²⁸Operation Safe Commerce was a public/private partnership developed after September 11, 2001, to improve supply chain security by testing security practices and commercially available technologies in an operational environment, including technologies for tracking and tracing containers, and sealing containers.

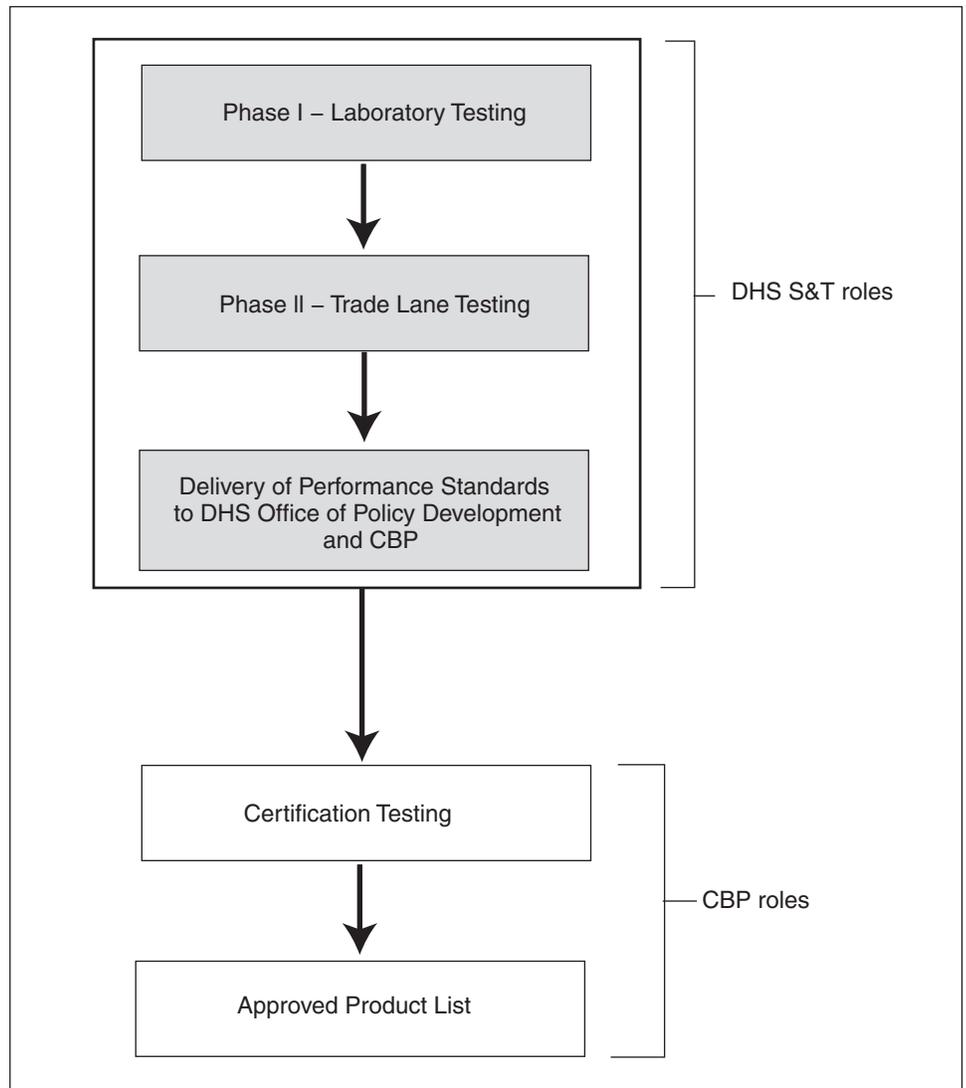
without triggering the alarm. Response protocols will need to be developed that include information on which parties are to respond to an alarm and the associated processes for responding. While CBP would likely respond to a container alarm by first scanning the container with NII equipment to mitigate any potential danger to a CBP officer entering the container to conduct a physical examination, CBP officers may not be nearby when an alarm occurs, particularly if it occurs during a container's transport to a foreign port, at a non-Container Security Initiative port, or while on a vessel in-transit. Furthermore, CBP will also need to consider whether foreign governments' customs agencies will be allowed access to the data generated by the technologies on containers departing their respective ports.

CBP Plans to Certify Technologies before They Can Be Used in the Supply Chain

Once a CONOPS is developed, certification testing can take place to determine the suitability of technologies consistent with the CONOPS. According to CBP officials, CBP plans to conduct certification testing to demonstrate whether technology products meet the performance standards issued by S&T and are suitable for implementation consistent with its operational concept. CBP officials stated they would begin the certification process by issuing a request for information seeking vendors to submit technologies for certification testing. Interested container security technology vendors would submit their products to CBP for certification testing, which consists of a mix of laboratory and trade lane testing to demonstrate whether the products meet the performance standards. According to CBP officials, they would determine a means to select vendor products for testing and then establish detailed methods to test and evaluate the technology products submitted by the vendors.

Office of Policy Development and CBP officials we spoke with anticipate certification testing would take approximately 3 to 4 months. The officials added that in advance of the testing, preparation time is needed to solicit participants from the trade industry and select trade lanes for testing. After conducting the tests, additional time will be needed to analyze the results to determine if the vendor's technology product will function as intended in the supply chain. If a technology product successfully completes certification testing, DHS will certify it as meeting its standards and the trade industry would be able to purchase it for use in the supply chain. Technologies that are successful during certification testing are expected to be implemented in the supply chain, according to an Office of Policy Development director. Figure 7 shows the process of developing an approved products list.

Figure 7: Certification Testing Process



Source: GAO analysis of DHS S&T information.

Conclusions

Container security technologies have the potential to contribute to CBP's layered security strategy by tracking containers, and detecting and reporting intrusions, while containers move through the supply chain. S&T has made progress in testing and evaluating certain container security technologies, and continues to work with vendors to develop these technologies, but challenges continue in finding technologies that can

provide intrusion detection through any of the six sides of a container. The ACSD project is not currently being funded due to the deficiencies identified during Phase I laboratory testing and the Hybrid Composite Container project is undergoing contract negotiations to resume work on the composite container after challenges were encountered with the vendor. In contrast, the CSD and MATTS projects—which will provide intrusion detection through container doors and a communications system, respectively—are nearing their completion and S&T expects to deliver performance standards to the Office of Policy Development and CBP by the end of 2010. Before delivering the performance standards, S&T must demonstrate that these container security technologies can work in the operational environments in which they are intended to be used. However, the operational environment testing that S&T plans to conduct is limited to the maritime environment and does not fully address the operational scenarios being considered by the Office of Policy Development and CBP. Until all intended operational scenarios are tested, S&T cannot provide reasonable assurance that the container security technologies would effectively function in all the operational scenarios identified by the Office of Policy Development and CBP for potential implementation. Conducting Phase II trade lane testing for the container security technologies in all intended operational scenarios would better position S&T to determine if the technologies will be suitable for use in their intended operational environments.

Recommendation for Executive Action

To ensure that the container security technologies being developed will function in their intended operational environments, we recommend that the Secretary of Homeland Security instruct the Assistant Secretary of the Office of Policy, the Commissioner of U.S. Customs and Border Protection, and the Under Secretary of the Science and Technology Directorate, to test and evaluate the container security technologies consistent with all of the operational scenarios DHS identified for potential implementation, before S&T provides performance standards to the Office of Policy Development and CBP.

Agency Comments

We provided draft copies of this report to the Secretaries of Homeland Security, Energy, and Defense for review and comments. DOE and DOD did not provide official written comments to include in the report. DHS provided official written comments, which are reprinted in appendix III. DHS concurred with our recommendation. In addition, DHS and CBP provided technical comments, which we incorporated as appropriate. In response to DHS's technical comments and subsequent discussion with

agency officials, we modified our recommendation to clarify its intent that DHS test and evaluate container security technologies consistent with all of the operational scenarios it has identified for potential implementation.

We are sending copies of this report to the Secretaries of Homeland Security, Energy, and Defense; and interested congressional committees. In addition, the report will be available on GAO's Web site at <http://www.gao.gov>.

If you or your staff members have any questions about this report, please contact Stephen L. Caldwell at (202) 512-9610 or Timothy M. Persons at (202) 512-6412, or by e-mail at caldwells@gao.gov or personst@gao.gov, respectively. 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 IV.

Sincerely yours,



Stephen L. Caldwell
Director, Homeland Security and Justice



Timothy M. Persons, Ph.D.
Chief Scientist
Director, Center for Science, Technology, and Engineering

Appendix I: Vendors Selected to Participate in Container Security Technology Projects

This appendix provides information on how the Department of Homeland Security's (DHS) Science and Technology (S&T) Directorate selected vendors to participate in the four container security technology projects. S&T used a multiple-round process to select vendors' technologies for development. Several vendors responded to S&T's 2004 broad agency announcement (BAA) for the Advanced Container Security Device (ACSD) project and 2003 small business innovative research (SBIR) solicitation for the Marine Asset Tag Tracking System (MATTS). Respondents' technology proposals were evaluated on their ability to meet the project requirements, and those considered to be viable were selected by S&T to participate in Round I. S&T selected vendors for subsequent rounds of development based on vendor performance and proposals. Vendor selection for the Container Security Device (CSD) project was based on the performance of prototypes during Round I of the ACSD project. Similarly, selection for the Hybrid Composite Container project was based on performance in the ACSD project. Table 7 provides information on the vendors selected to participate in each of the projects and the funds provided to the vendors.

Table 7: Selection and Funding of Vendors for Development of Container Security Technologies

Project name	Timeline of vendor selection	Funds provided to vendors (dollars in millions)	Number of vendor awards
Advanced Container Security Device (ACSD)	2004—BAA published	not applicable	30 respondents
	2005—Round I	\$3.4	5 awardees
	2006—Round II	6.1	2 awardees: L-3 Communications and SAIC
Container Security Device (CSD)	2006—Project initiated during Round II of ACSD project to provide interim door sensor capabilities while ACSD progressed	2.7	2 awardees: GTRI and SAIC (selected from the ACSD project)
Hybrid Composite Container	2005—Project initiated during ACSD project to provide ACSD capability in a composite container	5.8	2 awardees: Maine Secure Composites (composite container) and GTRI (sensor grid)
Marine Asset Tag Tracking System (MATTS)	2003—SBIR solicitation	not applicable	85 respondents
	2004—Round I	1.4	14 awardees
	2005—Round II	2.4	3 awardees
	2006—Round III	2.3	1 awardee: iControl, Inc.

Source: GAO analysis of DHS S&T information.

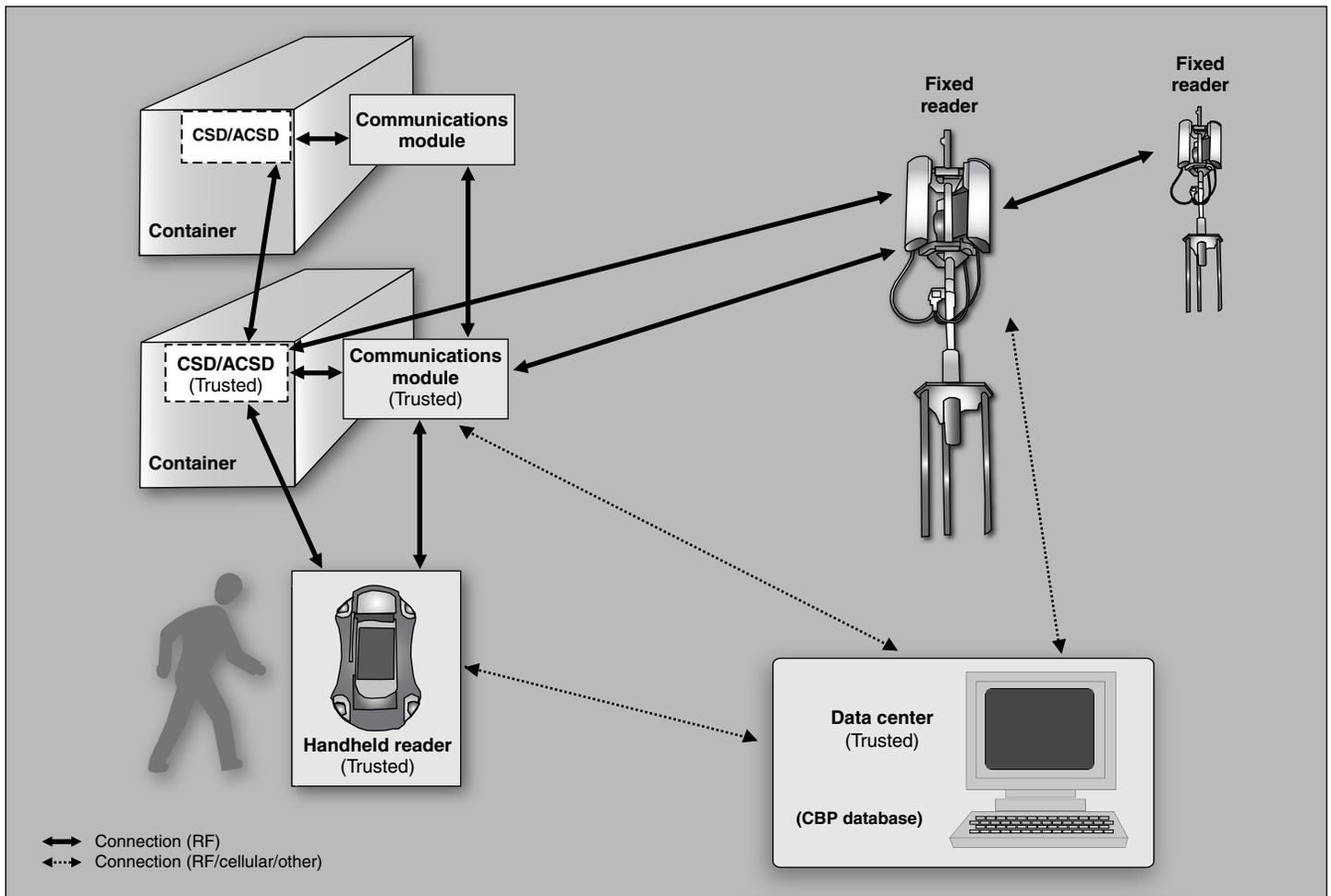
Appendix II: Description of Container Security Technologies' Communications Systems

Appendix II provides information on the communications system used to support container security technologies. Because ACSDs (including the sensor grid embedded in the Hybrid Composite Container) and CSDs are mounted inside of a container without a physical connection accessible from the outside of a closed container, a wireless communications system is to facilitate the remote arming (activating the intrusion detection capabilities) and disarming (deactivating the intrusion detection) of the ACSDs or CSDs. Furthermore, the communications system is to allow U.S. Customs and Border Protection (CBP) remote access to status information from an ACSD or CSD, including information about the health of the device and whether the device had detected an intrusion.

ACSDs and CSDs are intended to be a single component of a larger Security Device System, which may also include the following components (see fig. 8):

- **Communications Modules (CM):** These devices are mounted on the exterior of a container. A CM is to relay status information from an ACSD or CSD to a fixed status reader using radio frequency (RF) at 2.4 GHz or cellular communications. iControl, Inc. is developing a device known as the iTAG under the MATTS project to serve as a CM.
- **Fixed status readers:** These devices are to receive status information from ACSDs or CSDs located within 100 feet of the reader (or status updates relayed by a CM) and relay that status information using a variety of methods, such as RF, cellular, or Ethernet access, to a centralized data center. iControl, Inc., is developing a device known as the iGATE under the MATTS project to serve as a fixed status reader.
- **Handheld readers:** These are to be used by CBP or other authorized parties to receive status information from ACSDs or CSDs located within 10 feet of the reader.
- **Centralized data centers:** These centers are to receive status information from CMs and readers and allow CBP or other authorized parties to remotely monitor status information from all ACSDs and CSDs in the area served by the data center.

Figure 8: Security Device System Supporting Container Security Technology Communications



Source: GAO analysis of DHS S&T information.

ACSDs and CSDs should be able to communicate to a reader with or without the use of a CM. If no CM is mounted with an ACSD or CSD, the ACSD or CSD can communicate—by means of short-range RF at 2.4 GHz using communications capabilities on the ACSD or CSD itself—intrusion alerts and periodic general status updates to a fixed status reader located within 100 feet of the monitored container or to a handheld reader located within 10 feet of the monitored container. If a CM is associated with an ACSD or CSD, the ACSD or CSD can use short-range RF communications to relay messages through its CM to a more remote reader. If an ACSD or CSD needs to send status information to the data center while out of range of a reader, the external CM can attempt to relay the information through

other CMs mounted on nearby containers until a reader is in range. This relayed communications process is known as “meshing.” Similarly, if a reader is unable to communicate to the data center, it may attempt to pass messages to other nearby readers until communication with the data center is achieved.

Secure data generated by the ACSDs and CSDs are to be protected by translating the data into an unreadable form using a code (encryption). This encryption is to occur directly on the ACSDs and CSDs to avoid possible interception of confidential information transmitted during normal operation. Transmitted information includes security-related information used by CBP to determine the status of a container, but it may also include proprietary shipping information used by carriers or shippers (although such information must be encrypted separately). The encryption scheme also allows remote disarming of the devices (arming need not be done with an encrypted command), as only those devices with the encryption key will be capable of sending commands that the ACSDs or CSDs will recognize. The ACSDs, CSDs, handheld readers, and data centers (but not the fixed readers, as they are unattended and insecure) will be provided with the encryption key, allowing these components of the Security Device System to exchange information in a secure manner.

Communication of status information to remote readers for transfer to a data center is to occur, at minimum, at all points where reading is specified by DHS. These read points include the point of packing, the entrance gate at the port of departure, the exit gate at the port of arrival, and the entrance gate at the point of deconsolidation (where a container is unpacked). Communications should be designed in a nonproprietary format designed specifically for this application. This standard ensures that a Security Device System is permissible under all necessary international communications standards.

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

September 21, 2010

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

Dear Mr. Caldwell:

RE: Response to Draft Report GAO-10-887SU, *Supply Chain Security: To Ensure Effective Testing of Container Security Technologies, DHS Components Should Agree on How They Will Be Used (GAO 440824)*.

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report referenced above.

The Department of Homeland Security (DHS), including the Office of Policy (Policy), U.S. Customs and Border Protection (CBP) and Science and Technology (S&T), appreciates the investigative team's review of ongoing efforts to develop conveyance security technologies that can enhance the security of goods moving across our borders and traveling within our Nation. We appreciate the professionalism and subject matter expertise demonstrated by GAO's team members in conducting this review.

DHS concurs with the sole recommendation in this report that container security technologies should be tested and evaluated consistent with each of the intended operational scenarios before S&T provides performance standards to Policy and CBP. DHS agrees that identification of operational scenarios is a necessary prerequisite to the research and development process and the creation of performance standards; as discussed in the report, CBP, Policy, and S&T have identified a number of scenarios where technologies have the potential to be implemented in the future and therefore should be tested.

However, as a matter of additional clarification, DHS does not anticipate completion of testing in all possible operational scenarios prior to delivery of any container security technology performance standards to CBP and Policy. For example, the performance standards currently under development by S&T for a Container Security Device (CSD) reflect the first generation of such a device and are focused exclusively on maritime container routes. Phase II trade lane testing master plans, and any resulting performance standards, therefore will reflect only one of the many operational scenarios previously agreed upon within DHS. This 'phased approach' for delivery of performance standards to CBP and Policy will permit additional time and opportunity for consideration of potential implementation of these devices in specific, limited trade routes.

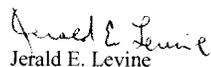
**Appendix III: Comments from the Department
of Homeland Security**

DHS remains committed to also pursuing technologies that will work within different types of routes in the air and sea environments, as well as inter-modally (for example, within or between a sea and land route). While a technology that works within a single mode of transport is a start, DHS acknowledges that the complexity and inter-connectedness of global supply chains and transportation systems necessitate more comprehensive solutions.

That said, DHS anticipates future work on CSD technologies for non-maritime routes or on devices that can be used even as goods transition between transportation systems in the coming years. The development, testing, and resulting performance standards will be based on the operational scenarios that have been identified to-date, as well as scenarios that may be proposed as our knowledge of supply chains continues to evolve. In fact, DHS is considering a pilot in Fiscal Year 2011 to evaluate potential applications for different types of container security technologies, including a CSD for non-maritime environments and the Marine Asset Tag Tracking System (MATTS) for several cross-border surface routes.

Once again, thank you for the opportunity to comment on this draft report. We look forward to working with you on future homeland security issues.

Sincerely,



Jerald E. Levine

Director

Departmental GAO/OIG Liaison Office

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Timothy M. Persons, (202) 512-6412 or personst@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Christopher Conrad and Richard Hung, Assistant Directors, and Lisa Canini, Analyst-in-Charge, managed this review. Leah Anderson, Alana Finley, Scott Fletcher, Adam Mirvis, and Matthew Tabbert made significant contributions to the work. In addition, Stanley Kostyla assisted with design and methodology; Frances Cook provided legal support; Katherine Davis and Lara Miklozek provided assistance in report preparation; and Pille Anvelt and Avy Ashery helped develop the report's graphics.

Glossary

The terms below are defined for the purposes of this GAO report.

Cargo

The freight (goods or products) carried by a vessel, barge, train, truck, or plane.

Concept of Operations (CONOPS)

A CONOPS is a user-oriented document that describes how an asset, system, or capability will be employed and supported from the users' viewpoint. A CONOPS also describes the operations that must be performed, who must perform them, and where and how the operations will be carried out.

Consolidator

The party who packs the container or arranges for the packing of the container.

Container

A box made of aluminum, steel, or fiberglass used to transport cargo by ship, rail, truck, or barge. Common dimensions are about 20 feet x 8 feet x 8 feet (called a TEU, or 20-foot-equivalent unit) or about 40 feet x 8 feet x 8 feet.

Customs

Government agency charged with enforcing the laws and rules passed to enforce the country's import and export revenues. In the United States these responsibilities are handled by U.S. Customs and Border Protection.

Customs Broker

The person who prepares the needed documentation for importing goods (just as a freight forwarder does for exports). In the United States, the broker is licensed under federal regulations to act on behalf of others in conducting transactions related to federal import and export requirements.

Exporter

A person or company that is responsible for the sending of goods out of one country to another.

Freight Forwarder

An individual or company that prepares the documentation and coordinates the movement and storage of export cargoes. See also **customs broker**.

Importer

A person or company that brings in goods from a foreign country.

Maritime Move

A one-way trip through the supply chain from stuffing to U.S. port of arrival on an ocean-going vessel.

Nonintrusive Inspection

Using technologies to scan the contents of a container without opening the container.

Non-vessel operating common carrier

A non-vessel operating common carrier buys space aboard a ship to get a lower volume rate and then sells that space to various small shippers, consolidates their freight, issues bills of lading, and books space aboard a ship.

Performance Standards

Requirements that must be met by products to ensure they will function as intended.

Physical Inspection

The opening of a container and removal of its contents for inspection.

Probability of Detection

The likelihood that a device will properly alarm when in the armed mode.

Probability of False Alarm

The likelihood that a device will improperly alarm, when in the armed mode, due to environmental conditions or conditions other than opening or removing the door(s).

Prototype

A functional preproduction version of a new type of product.

Red Teaming

Red teaming is performed from the perspective of an attacker with malevolent intentions, to identify and exploit weaknesses in a technology. The results of these tests allow for a better understanding of the risk associated with the corresponding device or system.

Scanning

Nonintrusively inspecting the contents of a container using technologies.

Screening

Assessing the security risk posed by a container based on available information.

Shipper

The person or company that is usually the supplier or owner of commodities shipped.

Supply Chain

The international network of retailers, distributors, transporters, storage facilities and suppliers that participate in the sale, delivery, and production of goods.

Trade Lane

A sea route ordinarily used by vessels.

Twenty-Foot Equivalent Unit (TEU)

A unit of measurement equal to the space occupied by a standard 20-foot container. Used in stating the capacity of container vessel or storage area. One 40-foot container is equal to 2 TEUs.

Vendor

An entity that develops container security technology prototypes.

Vessel

A ship or large boat.

Vessel Carrier

Any person or entity who, in a contract of carriage, undertakes to perform or to procure the performance of carriage by sea.

Vessel Manifest

Includes, among other things, a list of cargo being carried by the vessel.

Related GAO Products

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

Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps. [GAO-10-883T](#). Washington, D.C.: June 30, 2010.

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

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

Combating Nuclear Smuggling: DHS's Phase 3 Test Report on Advanced Portal Monitors Does Not Fully Disclose the Limitations of the Test Results. [GAO-08-979](#). Washington, D.C.: September 20, 2008.

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

Supply Chain Security: 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.

International Trade: Persistent Weaknesses in the In-Bond Cargo System Impede Customs and Border Protection's Ability to Address Revenue,

Trade, and Security Concerns. [GAO-07-561](#). Washington, D.C.: April 17, 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.

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

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.

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

Order by Phone

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

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

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

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

