



Report to the Chairwoman,
Subcommittee on Border and Maritime
Security, Committee on Homeland
Security, House of Representatives

February 2017

SUPPLY CHAIN SECURITY

Providing Guidance
and Resolving Data
Problems Could
Improve Management
of the Customs-Trade
Partnership Against
Terrorism Program

GAO Highlights

Highlights of [GAO-17-84](#), a report to the Chairwoman, Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The economic well-being of the United States depends on the movement of millions of cargo shipments throughout the global supply chain—the flow of goods from manufacturers to retailers or other end users. However, cargo shipments can present security concerns. CBP is responsible for administering cargo security and facilitating the flow of legitimate commerce. CBP has implemented several programs as part of a risk-based approach to supply chain security. One such program, C-TPAT, is a voluntary program in which CBP staff validate that members' supply chain security practices meet minimum security criteria. In return, members are eligible to receive benefits, such as a reduced likelihood their shipments will be examined.

This report assesses the extent to which (1) CBP is meeting its security validation responsibilities, and (2) C-TPAT members are receiving benefits. GAO reviewed information on security validations, member benefits, and other program documents. GAO also interviewed officials at CBP headquarters and three C-TPAT field offices chosen for their geographical diversity; as well as select C-TPAT members and trade industry officials.

What GAO Recommends

GAO is recommending that CBP develop (1) standardized guidance for field offices regarding the tracking of information on security validations, and (2) a plan with milestones and completion dates to fix the Dashboard so the C-TPAT program can produce accurate data on C-TPAT member benefits. DHS concurred with GAO's recommendations.

View [GAO-17-84](#). For more information, contact Jennifer Grover at (202) 512-7141 or Groverj@gao.gov.

February 2017

SUPPLY CHAIN SECURITY

Providing Guidance and Resolving Data Problems Could Improve Management of the Customs-Trade Partnership Against Terrorism Program

What GAO Found

Staff from U.S. Customs and Border Protection's (CBP) Customs-Trade Partnership Against Terrorism (C-TPAT) program have faced challenges in meeting C-TPAT security validation responsibilities because of problems with the functionality of the program's data management system (Portal 2.0). In particular, since the system was updated in August 2015, C-TPAT staff have identified instances in which the Portal 2.0 system incorrectly altered C-TPAT members' certification or security profile dates, requiring manual verification of member data and impairing the ability of C-TPAT security specialists to identify and complete required security validations in a timely and efficient manner. While the focus of CBP's staff was initially on documenting and addressing Portal 2.0 problems as they arose, the staff have begun to identify root causes that led to the Portal 2.0 problems. For example, CBP staff cited unclear requirements for the system and its users' needs, coupled with inadequate testing, as factors that likely contributed to problems. In response, CBP staff have outlined recommended actions, along with timeframes for completing the actions. The staff stated that they will continue to work on identifying and addressing potential root causes of the Portal problems through 2017. C-TPAT officials told us that despite the Portal 2.0 problems, they have assurance that required security validations are being tracked and completed as a result of record reviews taking place at field offices. However, these field office reviews were developed in the absence of standardized guidance from C-TPAT headquarters. While the current validation tracking processes used by field offices do account for security validations conducted over the year, standardizing the process used by field offices for tracking required security validations could strengthen C-TPAT management's assurance that its field offices are identifying and completing the required security validations in a consistent and reliable manner.

CBP cannot determine the extent to which C-TPAT members are receiving benefits because of data problems. Specifically, since 2012, CBP has compiled data on certain events or actions it has taken regarding arriving shipments—such as examination and hold rates and processing times—for both C-TPAT and non-C-TPAT members through its Dashboard data reporting tool. However, on the basis of GAO's preliminary analyses and subsequent data accuracy concerns cited by C-TPAT program officials, GAO determined that data contained in the Dashboard could not be relied on for accurately measuring C-TPAT member benefits. Also, CBP has likely relied on such questionable data since it developed the Dashboard in 2012, and, thus, cannot be assured that C-TPAT members have consistently received the benefits that CBP has publicized. C-TPAT officials stated that they are analyzing the Dashboard to finalize an action plan to correct the data concerns. It is too soon to tell, though, whether this process will fully address the accuracy and reliability issues. Despite these issues, C-TPAT officials are exploring new member benefits, and industry officials we met with generally spoke positively of the C-TPAT program.

Contents

Letter		1
	Background	5
	CBP Is Taking Steps to Resolve Data System Problems, but Could Take Additional Steps to Ensure Staff Meet Security Validation Responsibilities	13
	CBP Cannot Determine the Extent to Which C-TPAT Members Are Receiving Benefits Because of Data Concerns	18
	Conclusions	23
	Recommendations for Executive Action	24
	Agency Comments and Our Evaluation	24
Appendix I	Further Details on the Customs-Trade Partnership Against Terrorism (C-TPAT) Member Screening Process	26
Appendix II	Comments from the Department of Homeland Security	29
Appendix III	GAO Contact and Staff Acknowledgments	32
Tables		
	Table 1: Types of Entities Eligible for Customs-Trade Partnership Program Against Terrorism (C-TPAT) Membership and Their Role in the Supply Chain	6
	Table 2: Benefits Offered to Members of the Customs-Trade Partnership Against Terrorism (C-TPAT)	11
Figures		
	Figure 1: Example of Key Points in the Global Supply Chain	6
	Figure 2: Percentage of Customs-Trade Partnership Against Terrorism (C-TPAT) Members, by Industry Type, as of September 2016	8
	Figure 3: Overview of the Customs-Trade Partnership Against Terrorism (C-TPAT) Member Screening Process	10

Abbreviations

AQUA	Advanced Qualified Unlading Approval
ATS	Automated Targeting System
CBP	Customs and Border Protection
CEE	Center for Excellence and Expertise
COAC	Advisory Committee on Commercial Operations to U.S. Customs and Border Protection
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
FAST	Free and Secure Trade
ISA	Importer Self-Assessment
MRA	Mutual Recognition Arrangement
PMBOK® Guide	<i>A Guide to the Project Management Body of Knowledge</i>
SAFE Port Act	Security and Accountability for Every Port Act of 2006
SAFETY Act	Support Anti-terrorism by Fostering Effective Technologies Act of 2002
TASPD	Targeting and Analysis Systems Program Directorate

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.



February 8, 2017

The Honorable Martha McSally
Chairwoman
Subcommittee on Border and Maritime Security
Committee on Homeland Security
House of Representatives

Dear Madam Chairwoman

The economic well-being of the United States is dependent on the expeditious flow of millions of cargo shipments that arrive each year by land, sea, or air.¹ Cargo shipments are an important segment of the global supply chain—the flow of goods from manufacturers to retailers or other end users—and can present significant security concerns. Within the federal government, U.S. Customs and Border Protection (CBP), part of the Department of Homeland Security (DHS), is responsible for administering cargo security and reducing the vulnerabilities associated with the supply chain, while facilitating the flow of legitimate commerce. Balancing security concerns with the need to facilitate the free flow of commerce remains an ongoing challenge for the public and private sectors alike.²

CBP has implemented several programs as part of a layered, risk-informed approach to supply chain security. The Security and Accountability for Every Port Act of 2006 (SAFE Port Act)³ established a statutory framework for key programs within CBP's layered security strategy that previously had not specifically been required by law. One such program, the Customs-Trade Partnership Against Terrorism (C-TPAT), began in November 2001 and is a voluntary program in which CBP officials work with private companies to review and validate their

¹A shipment is the tender of one lot of cargo at one time from one shipper to one recipient. In some cases, a shipment will refer to all the contents in a single shipping container. In other cases, a shipment may refer to the cargo in multiple containers. Additionally, a single container could hold multiple shipments from different supply chain parties.

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

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

supply chain security practices, as well as the security practices of the companies or entities in their global supply chains, to ensure they meet a set of minimum security criteria defined by CBP.⁴ In return for ensuring their supply chain security practices meet CBP's minimum security criteria, C-TPAT members are eligible to receive various benefits, such as reduced scrutiny or expedited processing of their U.S.-bound shipments. According to C-TPAT officials, as of September 2016, there were 11,490 C-TPAT members, whose collective shipments have accounted for over half of all cargo by value entering the United States in recent years.

We previously reviewed and reported on the C-TPAT program in 2008.⁵ At that time we found that, among other things, CBP faced challenges in verifying that C-TPAT members' security practices met CBP's minimum criteria, and CBP's records management system did not identify interim processing dates that would enable management or others to determine CBP's compliance with program requirements. We recommended that CBP improve the security validation process, enhance its records management system, and identify opportunities to establish performance measures for improving supply chain security. CBP concurred with and has since implemented the recommendations.

Given the importance of the C-TPAT program and its continued growth in membership, you asked that we review the C-TPAT program. In particular, this report addresses the following questions:

1. To what extent is CBP meeting its security validation responsibilities?
2. To what extent are C-TPAT members receiving benefits?

To address the first objective, we requested data from C-TPAT's Portal 2.0, the data system designed to maintain C-TPAT program data—such as members' certification, security validation, and revalidation records—with the intent of reviewing the data to determine CBP's timeliness and completeness in meeting its security validation responsibilities.⁶ However,

⁴Pub. L. No. 109-347, §§ 211-23, 120 Stat. 1884, 1909-15 (codified at 6 U.S.C. §§ 961-73) (establishing the C-TPAT program in statute).

⁵GAO, *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).

⁶Portal 2.0 is an information-sharing and data management system used by C-TPAT officials to review C-TPAT member-submitted information and record certification and validation information. C-TPAT member companies use the Portal to submit program applications, security profiles, and other information to C-TPAT officials.

based on discussions with C-TPAT managers, as well as staff members responsible for maintaining the Portal 2.0 system, we determined that data from the system were not reliable because of functionality problems, as discussed in more detail later in the report. We also obtained and reviewed CBP documentation describing Portal 2.0 system requirements, its development, the nature of Portal 2.0 problems C-TPAT staff have experienced, and actions that CBP staff are taking to address these problems. Further, we conducted interviews with officials from the C-TPAT program and CBP's Office of Information Technology at CBP headquarters, as well as C-TPAT field office directors, supply chain security specialists (hereafter referred to as "security specialists"), and their supervisors at three of C-TPAT's six field offices in Los Angeles, California; New York, New York; and Houston, Texas.⁷ These interviews provided us with additional information about the Portal 2.0 problems and the extent to which the problems have affected the security specialists' efforts to (1) determine which C-TPAT members are due for security validations or revalidations, (2) conduct those security validations or revalidations, and (3) document the results. While the information gathered from these site visits cannot be generalized to all C-TPAT field office directors and security specialists, they provide insights into the nature of the validation process and use of Portal 2.0 in conducting security validations. We reviewed documentation and interviewed agency officials to determine how C-TPAT officials assured that security validations were identified and conducted, as needed, following the Portal 2.0 system problems that occurred in 2015. We also gathered information on how C-TPAT headquarters officials solicit and review the field office director security validation submissions and compared this process to best practices on control activities, information, communication, and monitoring as identified in *Standards for Internal Control in the Federal Government*.⁸ We then reviewed CBP and C-TPAT's efforts to test Portal 2.0 prior to deploying it and to address Portal 2.0 problems that have arisen since it was deployed in August 2015. Finally, we interviewed a representative from the Advisory Committee on Commercial Operations to U.S. Customs and Border Protection (COAC) and a nongeneralizable sample of trade industry association officials and C-TPAT members selected to reflect a variety of different C-TPAT member industry types

⁷We selected these offices to provide geographic representation from C-TPAT offices located on the West Coast, East Coast, and Gulf Coast, respectively.

⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

(e.g., importers, highway carriers) to obtain their perspectives on security validation and revalidation procedures; as well as any potential areas for improvement for the C-TPAT program.

To address the second objective, we obtained and analyzed data compiled by CBP on examination rates, hold rates, and average processing times of cargo shipments from C-TPAT members as compared to cargo shipments from non-C-TPAT members covering fiscal years 2011 through 2015, the 5 most recent fiscal years for which these data were available.⁹ In analyzing these data, we discovered that they were not reliable for the purpose of reporting on the actual benefits received by C-TPAT members, which we discuss in more detail later in the report. After determining that the data were not reliable, we interviewed cognizant CBP staff to explore the extent to which C-TPAT officials had determined the causes of the data reliability issues and had devised solutions. We compared the evidence we compiled to criteria on effective information management practices identified in *Standards for Internal Control in the Federal Government*,¹⁰ leading project management practices identified in the Program Management Institute's *A Guide to the Project Management Body of Knowledge*,¹¹ and requirements of the SAFE Port Act. In addition, we reviewed information describing C-TPAT benefits for which C-TPAT does not systematically gather data because the benefits are difficult to quantify—such as access to C-TPAT security specialists—as well as information on efforts to potentially expand benefits provided to C-TPAT members. We supplemented our data analyses and document reviews with testimonial evidence gathered through interviews with C-TPAT officials at CBP

⁹An examination refers to either (1) the scanning of a container or other cargo conveyance using large-scale non-intrusive inspection technology, which may use X-rays or gamma rays to create an image of the contents of the container or other conveyance; or (2) a physical inspection of a container or other cargo conveyance. CBP can place a hold on cargo shipments from leaving the terminal for a number of reasons, such as when the shipment has been identified by CBP's targeting software as high-risk, or CBP targeters have questions regarding shipment information they want to resolve. Average processing time refers to the difference between the date and time of a shipment's arrival (or placement on hold) and the date and time at which it was released.

¹⁰[GAO-14-704G](#).

¹¹Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, 2013. PMBOK is a trademark of Project Management Institute, Inc. The PMBOK® Guide describes standard project management practices such as, among other things, the need to establish project objectives and a plan of action via a project schedule with major milestones.

headquarters, as well as C-TPAT field office directors, supervisory security specialists, and security specialists at the three C-TPAT field offices mentioned earlier. We also interviewed officials in CBP's Office of Information Technology to discuss how C-TPAT benefit data were compiled, as well as officials from the trade industry associations and C-TPAT members mentioned above to discuss their views on C-TPAT program operations and benefits. While their views cannot be generalized to the entire population of C-TPAT members, they do provide insights into members' perspectives on C-TPAT program benefits and challenges.

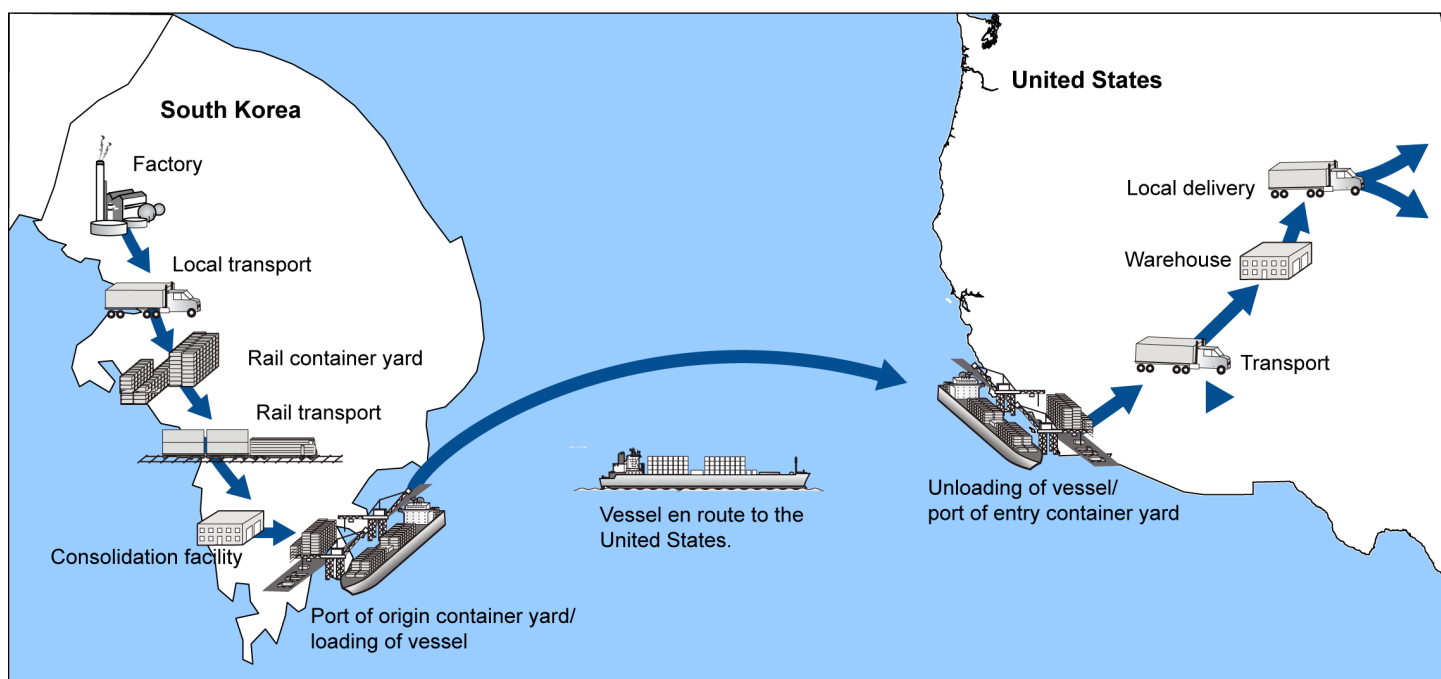
We conducted our work from September 2015 to February 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Global Supply Chain

Supply chain security is a principal element of CBP's layered strategy to protect commerce. In the post-9/11 environment, the movement of cargo shipments throughout the global supply chain from foreign manufacturers, suppliers, or vendors to retailers or other end users in the United States is inherently vulnerable to terrorist actions. Every time responsibility for cargo shipments changes hands along the global supply chain there is the potential for a security breach. Thus, vulnerabilities exist that terrorists could exploit by, for example, placing a weapon of mass destruction into a container for shipment to the United States or elsewhere. Figure 1 illustrates key points of transfer involved in the global supply chain—from the time that a shipment is loaded with goods at a foreign factory to its arrival at the U.S. port and ultimately the retail facility or end user.

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



Source: GAO; Map Resources (map). | GAO-17-84

C-TPAT Program Structure and Membership

CBP initiated the C-TPAT program in November 2001 as part of its layered strategy for overseeing global supply chain security. C-TPAT aims to secure the flow of goods bound for the United States through voluntary antiterrorism partnerships with entities that are stakeholders within the international trade community—see table 1 for information on the types of entities eligible for C-TPAT membership.

Table 1: Types of Entities Eligible for Customs-Trade Partnership Program Against Terrorism (C-TPAT) Membership and Their Role in the Supply Chain

C-TPAT member type	Role in the supply chain
Air/rail/sea carriers	Carriers transport cargo from foreign nations into the United States via air, rail, or sea.
Border highway carriers (U.S./Canada or U.S./Mexico)	Highway carriers transport cargo for scheduled and unscheduled operations via road across the Canadian and Mexican borders.
Consolidators	Consolidators combine cargo from a number of shippers that will deliver the goods to several buyers. In C-TPAT, this includes entities that do not necessarily physically handle freight, but work to facilitate its movement through carrier bookings, generation of bills of lading, or coordination with carriers.
Exporters	Entities that actively export cargo from the United States to another country.
Foreign manufacturers	Entities located in Canada or Mexico that produce goods for sale to the United States.

C-TPAT member type	Role in the supply chain
Importers	In the course of trade, importers bring articles of trade from a foreign source into a domestic market.
Licensed U.S. customs brokers	Brokers clear goods through customs. The responsibilities of a broker include preparing and filing an entry form, advising the importer on duties to be paid, and arranging for delivery of the goods to the importer.
Mexican Long Haul Highway Carriers	Companies that haul cargo within Mexico destined for the United States, but do not cross the United States/Mexico border.
Third Party Logistics Providers	Provide outsourced logistics services to other entities for part or all of their supply chain management functions. These services typically include integrated warehousing, transportation services, and customs and freight consolidation.
U.S. or Foreign-Based Marine Port or Terminal Operators	Port authorities are entities of state or local governments that own, operate, or otherwise provide wharf, dock, and other marine terminal investments at ports. Terminal operator responsibilities include the overseeing and unloading of cargo from ship to dock, checking the actual cargo against the ship's manifest (list of goods), checking documents authorizing a truck to pick up cargo, and overseeing the loading and unloading of railroad cars.

Source: GAO analysis of information provided by CBP. | GAO-17-84

The SAFE Port Act established a statutory framework for the C-TPAT program.¹² In addition to formally establishing C-TPAT as a voluntary government-private sector partnership program to strengthen and improve the overall security of the global supply chain, the act codified existing membership processes for the C-TPAT program and added new components, such as time frames for certifying, validating, and revalidating members' security practices.

Through C-TPAT, CBP intends to enhance the security of the global supply chain to the United States through partnership agreements, and by reviewing and periodically validating C-TPAT members' security practices. As a first step in C-TPAT membership, an entity must sign an agreement with CBP signifying its commitment to enhance its supply chain security practices consistent with C-TPAT minimum security criteria and to work to enhance security throughout its global supply chain to the United States.¹³ The partnership agreements that C-TPAT members sign

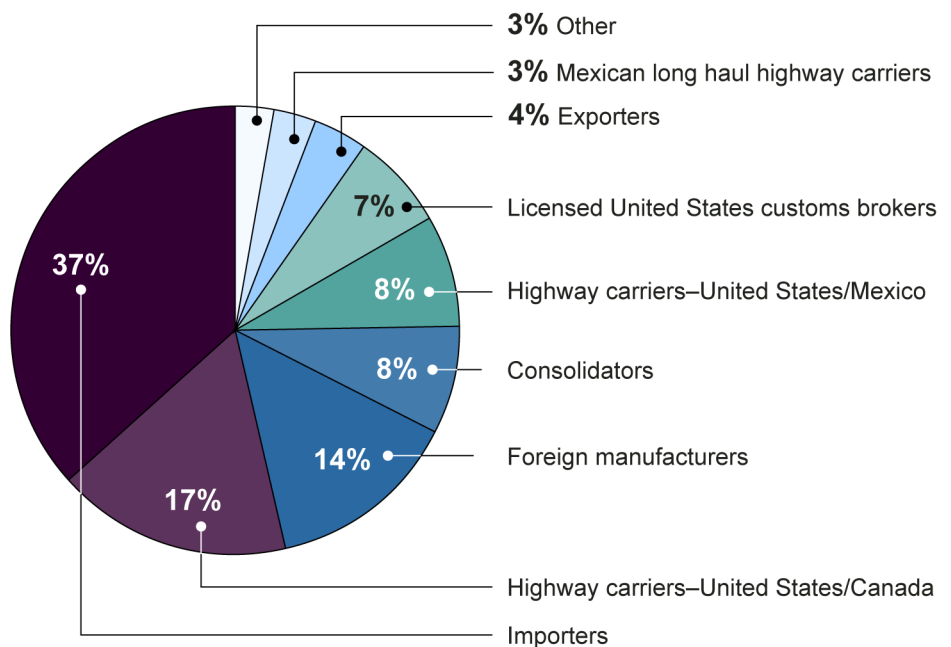
¹²Pub. L. No. 109-347, §§ 211-23, 120 Stat. 1884, 1909-15 (codified at 6 U.S.C. §§ 961-73).

¹³For example, to address the C-TPAT minimum security criteria, C-TPAT importers must, among other things, ensure that their global supply chain partners are either C-TPAT certified or demonstrate that they meet C-TPAT security criteria; have written procedures on how container seals (locking devices used to secure containers) are to be controlled and affixed to loaded containers; and employ access controls to prevent unauthorized entry to facilities.

provide CBP with the authority it needs to validate members' security practices.

According to CBP officials, as of September 2016, there were 11,490 C-TPAT members. Importers, representing 37 percent of the C-TPAT members, were the largest C-TPAT member group and, as shown in Figure 2, the remaining 63 percent of C-TPAT members were distributed among other trade industry sectors. Since we last reported on the C-TPAT program in April 2008, CBP has expanded C-TPAT membership to include other trade industry sectors, such as third party logistics providers and exporters.

Figure 2: Percentage of Customs-Trade Partnership Against Terrorism (C-TPAT) Members, by Industry Type, as of September 2016



Source: GAO analysis of data provided by CBP. | GAO-17-84

Note: Totals do not add up to 100 percent due to rounding. "Other" industry types are Third Party Logistics Providers, Sea Carriers, U.S. Marine Port or Terminal Operators, Air Carriers, Rail Carriers, and Foreign-Based Marine Port Terminal Operators. Each of these other industry types individually represent less than one percent of total membership.

According to CBP officials, as of September 2016, CBP employed 146 security specialists (to include supervisory security specialists) who are to certify or validate members' security practices and provide other services for C-TPAT members, such as serving as points of contact concerning C-

TPAT program responsibilities. The security specialists operate from C-TPAT headquarters in Washington, D.C., and six field offices throughout the United States: Los Angeles, California; Miami, Florida; Newark, New Jersey; Buffalo and New York, New York; and Houston, Texas. The C-TPAT program, which resides within CBP's Office of Field Operations (OFO), was funded at over \$36 million in fiscal year 2016.¹⁴

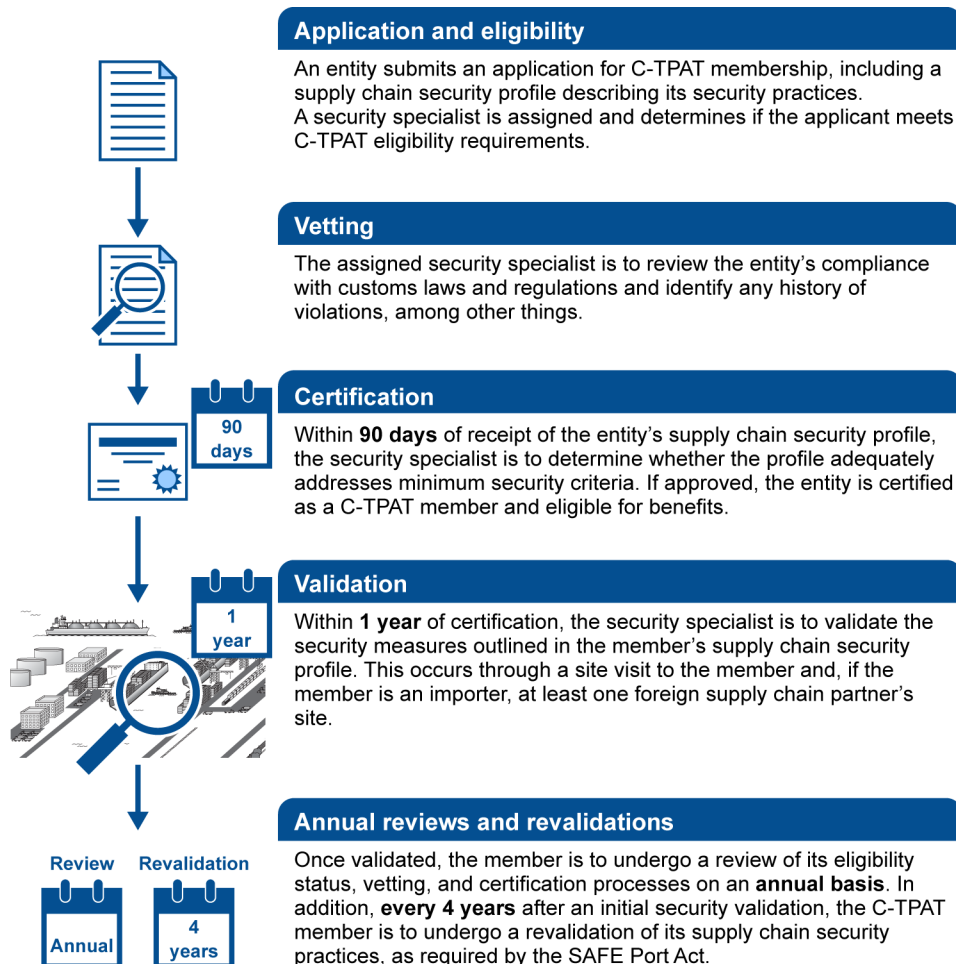
C-TPAT Membership Requirements and Benefits

CBP employs a multistep process, led by its security specialists, for accepting entities as members in the C-TPAT program, validating their supply chain security practices—to include the practices of their supply chain partners—and providing them benefits.¹⁵ This screening process, which CBP has documented through standard operating procedures, consists of five key steps, as shown in figure 3 and described in greater detail in appendix I.

¹⁴Department of Homeland Security, *Congressional Budget Justification*, FY 2017-Volume I.

¹⁵In some instances, a member's foreign supply chain partners may have undergone a type of security validation conducted in its home country. CBP may accept this validation in lieu of conducting its own if the member's validation was conducted by a foreign customs administration with which CBP has a Mutual Recognition Arrangement (MRA). MRAs are arrangements with foreign customs administrations that allow the security-related practices and programs taken by the customs or maritime security administration of one partner to be recognized and accepted by the administration of another. MRAs can be entered into with the customs administrations of other countries or other governing bodies, such as the European Union, that have a Customs Mutual Assistance Agreement (which allow for the exchange of information, intelligence, and documents that will assist countries in the prevention and investigation of customs offenses) in place and in force with the United States. As of the end of fiscal year 2016, CBP had MRAs in place with 11 foreign countries or governing bodies: New Zealand, Canada, Jordan, Japan, Korea, the European Union, Taiwan, Israel, Mexico, Singapore, and the Dominican Republic.

Figure 3: Overview of the Customs-Trade Partnership Against Terrorism (C-TPAT) Member Screening Process



Source: GAO analysis of CBP information. | GAO-17-84

To facilitate the member screening process, C-TPAT staff gather, review, and prepare documentation using an information-sharing and data management system called Portal 2.0. C-TPAT officials use Portal 2.0 to review C-TPAT member-submitted information and record certification and validation results. In addition, C-TPAT member companies use Portal 2.0 to submit program applications, security profiles, and other information to C-TPAT officials.

In exchange for allowing C-TPAT staff to review and validate their supply chain security practices, C-TPAT members become eligible to receive

benefits—such as reduced likelihood of examinations of their shipments, expedited shipment processing, and greater access to CBP staff and information—once their membership is certified. Upon certification, C-TPAT importers and exporters only are granted Tier I status. Importers and exporters whose supply chain security practices have been validated by C-TPAT security specialists are granted either Tier II (meeting minimum security criteria for their business type) or Tier III (employing innovative supply chain security measures that are considered best practices and exceed minimum security criteria) status.¹⁶ Tier II and Tier III C-TPAT importers and exporters receive increasingly reduced risk scores (i.e., as tier level increases, risk scores are lowered) in CBP’s Automated Targeting System (ATS), thus generally reducing the likelihood that their shipments will be examined upon entering U.S. ports.¹⁷ Specific benefits offered to C-TPAT members, as listed in CBP’s *C-TPAT Program Benefits Reference Guide*, can be found in Table 2.

Table 2: Benefits Offered to Members of the Customs-Trade Partnership Against Terrorism (C-TPAT)

C-TPAT member benefit	Description
Reduced examination rates for C-TPAT importers	C-TPAT members have their assigned risk scores in U.S. Customs and Border Protection’s (CBP) Automated Targeting System (ATS) lowered based on C-TPAT membership and Tier level.
Access to the Free and Secure Trade (FAST) lanes	FAST lanes are dedicated highway lanes available to C-TPAT members at many Canada/Mexico land border ports of entry, allowing expedited border crossing privileges to those C-TPAT highway carriers that are validated.
Front of the line processing	To the extent possible and practicable, C-TPAT shipments subject to an examination are moved ahead of any non-C-TPAT shipments, so members’ shipments would not spend as much time awaiting examinations.
Business resumption	In the event of a significant disruption or delay in CBP cargo processing operations, CBP takes actions to maintain communication and coordination with C-TPAT members, and priority is given to processing C-TPAT member shipments (after processing shipments designated as national priority goods).

¹⁶According to CBP, leading practices for an entity seeking C-TPAT membership would be that it provides for a system of checks, balances, and accountability for security measures throughout its global supply chain. These security measures could include, among other things, having employee photos displayed on monitors as they enter a building so that security guards can verify their identity, and conducting semi-annual security awareness training for its supply chain business partners.

¹⁷ATS is a web-based decision support system that includes a set of rules to assess the risk level for each arriving cargo shipment. While a lower ATS score generally reduces the likelihood of an examination for a shipment, CBP officers may choose to examine shipments for any reasons they deem necessary.

C-TPAT member benefit	Description
Expedited trade processing	C-TPAT members are given priority consideration by the Centers of Excellence and Expertise (CEEs) in the resolution of any trade compliance and admissibility issues occurring at ports of entry. ^a
Access to a C-TPAT Supply Chain Security Specialist	Each C-TPAT member is assigned a security specialist who manages the member's C-TPAT relationship with CBP. Also, the security specialist is available to assist members with issues related to supply chain security and to answer questions and concerns related to CBP.
Access to the C-TPAT Portal system	C-TPAT's automated Portal system allows members to communicate with CBP and exchange program-related information in a secure manner. The Portal also houses a public information library containing materials that cover training and supply chain security best practices.
Eligibility to attend C-TPAT's annual conference	C-TPAT members are eligible to attend C-TPAT conferences and other training seminars.
Eligibility to participate in the Importer Self-Assessment (ISA) program	ISA is a voluntary approach to trade compliance which allows qualified importers to assess and monitor their own compliance with CBP's laws and regulations in exchange for specific benefits, such as exemption from comprehensive compliance audits.
Stratified exam benefit for importer partners ^b	C-TPAT Tier II and Tier III importers that also participate in the Importer Self-Assessment program are eligible for special accommodations under the stratified examination process.
Penalty mitigation	This benefit is offered to members for late submission of data required under the Importer Security Filing requirements.
Eligibility to other programs	C-TPAT membership opens eligibility to other federal government pilot programs, such as the Food and Drug Administration's Secure Supply Chain program, which requires U.S. importers to be C-TPAT certified at the Tier II or Tier III levels.

Source: Information provided by CBP. | GAO-17-84

Note: C-TPAT importers and exporters whose security practices have been validated by C-TPAT staff as meeting minimum security criteria are granted Tier II status, and those that employ security practices that C-TPAT staff validate as exceeding minimum security criteria are granted Tier III status. In addition to the benefits in the above table that were identified in the C-TPAT Program Benefits Reference Guide, C-TPAT Tier III importers are also eligible for legal liability protections under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). See Pub. L. No. 107-296, tit. VIII, subtit. G, §§ 861-65, 116 Stat. 2135, 2238-42 (codified at 6 U.S.C. §§ 441-444). The SAFETY Act Program is intended to encourage the development and deployment of effective anti-terrorism products and services by providing liability protections to companies that deploy qualified anti-terrorism technologies to defend against, respond to, or recover from an act of terrorism. In 2014, the DHS Science and Technology Directorate—which manages the program—approved a block designation granting these benefits to C-TPAT Tier III members who choose to apply to the program, and also allows these members to receive expedited processing of the SAFETY Act application.

^aCEEs were formed by CBP to facilitate the entry of merchandise imported by entities within certain industries, and can make entry processing recommendations to ports for shipments in those industries. There are currently ten CEEs representing ten industries at specific locations throughout the United States. CEEs also serve as resources to the broader trade community and U.S. government partners by answering questions, providing information, and developing trade facilitation strategies.

^bUnder the stratified exam benefit, if an importer has an arriving shipment consisting of multiple containers, but only one container is targeted for examination, the importer may move the remaining containers from that shipment to its premises. As such, these remaining containers are exempt from being held by CBP while CBP staff examine the targeted container. The exempt containers that are released are to remain sealed and available for inspection contingent upon the result of the examination of the targeted container. Conversely, for non-C-TPAT members undergoing a stratified

exam, the unexamined containers are to remain at the port until the examination of the targeted container is completed.

While C-TPAT membership can reduce the probability of CBP selecting members' shipments for examinations, holds, or other enforcement actions, CBP maintains the authority to conduct appropriate enforcement actions. In addition, other federal agencies (e.g., U.S. Department of Agriculture, Food and Drug Administration, etc.) can conduct inspections of arriving cargo shipments based on their own selection criteria.

CBP Is Taking Steps to Resolve Data System Problems, but Could Take Additional Steps to Ensure Staff Meet Security Validation Responsibilities

Data System Problems Have Led to Challenges in Identifying and Completing C-TPAT Member Security Validations

C-TPAT staff have faced challenges in meeting C-TPAT security validation responsibilities in an efficient and timely manner because of problems with the functionality of C-TPAT's data management system (Portal 2.0). In particular, while the intended purpose of transitioning from Portal 1.0 to Portal 2.0 in August 2015 was to improve functionality and facilitate communication between security specialists and C-TPAT members, a series of problems arose as a result of this transition that have impaired the ability of C-TPAT staff to identify and complete required C-TPAT member certification procedures and security profile reviews in a timely and efficient manner. For example, C-TPAT field office directors, supervisory security specialists, and security specialists we met with identified numerous instances in which the Portal 2.0 system incorrectly altered C-TPAT members' certification or security profile dates. In particular, when C-TPAT officials transferred responsibility for some C-TPAT members' accounts from one security specialist to another, those members' certification dates were sometimes incorrectly changed. These altered dates, in turn, have interfered with security specialists' ability to properly identify and track which member companies are due for an annual security profile review.

In addition to the impact they have had on the daily responsibilities of security specialists, Portal 2.0 problems also made it more difficult for C-TPAT managers to complete the C-TPAT program's 2016 annual work plan for assigning responsibilities for member security validations and revalidations to its security specialists. C-TPAT managers have typically relied on data from Report Builder, a reporting module within Portal, to develop annual work plans.¹⁸ However, in November 2015, C-TPAT staff had difficulty using Report Builder to access historical data from Portal 1.0 that were to have migrated to Portal 2.0 regarding C-TPAT members that were due to have security validations or revalidations conducted in 2016. As a result, the initial 2016 work plan did not have accurate data on the number of C-TPAT members due for security validations or revalidations. In addressing this issue, C-TPAT's Director pointed out that while the Portal is intended to facilitate the ability of security specialists to perform their responsibilities, each security specialist is experienced and is not to rely solely on the Portal to complete his or her job responsibilities. So, to complete the 2016 work plan, C-TPAT managers implemented a requirement for security specialists in each of C-TPAT's six field offices to manually review documentation, such as prior security validation reports, for each of their assigned members (approximately 80 to 100 members per security specialist) to verify or correct the certification and security validation dates recorded in Portal 2.0 and to ensure that the 2016 work plan identified all members due for security validations or revalidations in 2016. C-TPAT officials then used the information gathered through these additional manual steps to update and correct the 2016 work plan.

Further, security specialists we met with told us that they had difficulty saving and submitting security validation reports to C-TPAT managers in a timely manner because of Portal 2.0 problems. Instead of submitting the validation reports directly through the Portal, security specialists told us they sometimes had to prepare draft security validation reports offline and copy and paste information section by section in order for Portal 2.0 to accept and save the security validation reports. While these alternate means of verifying validation responsibilities and mitigating Portal 2.0 problems have generally allowed security specialists to complete their required annual security profile reviews and validations, the security specialists stated that these work arounds are time consuming and have

¹⁸Report Builder is the primary tool C-TPAT management uses to query information from Portal records to generate a list of accounts that are required to be validated or revalidated for a given year. The tool is also to be used to verify compliance with SAFE Port Act requirements and to track C-TPAT program performance.

necessitated the use of overtime. The C-TPAT Director acknowledged the problems her staff have experienced with Portal 2.0 and that these problems have led to some inefficient work practices.

Problems with Portal 2.0 have also had an adverse impact on C-TPAT members. For example, security specialists told us that some C-TPAT members have experienced difficulties viewing validation report findings because of problems in accessing Portal 2.0. If validation reports contain findings regarding security practices that fail to meet the minimum security criteria that members are to address, the members are to respond to C-TPAT staff within 90 days about their plans for addressing the findings and improving their supply chain security practices to meet CBP's minimum security criteria. Because Portal 2.0 problems have sometimes prevented C-TPAT members from accessing and responding to validation reports in a timely manner, C-TPAT managers told us they have needed to grant these members additional time to respond to validation report findings.

CBP Staff Are Taking Steps to Address Data System Problems

CBP staff from the C-TPAT program and the Office of Information Technology's Targeting and Analysis Systems Program Directorate (TASPD) have taken steps to address problems with Portal 2.0. When problems with Portal 2.0 first surfaced in August 2015, Portal users in the C-TPAT field offices began recording problems in spreadsheets. C-TPAT headquarters officials collected these spreadsheets and sent them to TASPD managers to address. In an effort to improve coordination and communication between C-TPAT and TASPD staff, in February 2016, CBP officials developed a more centralized and systematic process for documenting, prioritizing, and addressing Portal 2.0 problems as they arise. In particular, a single C-TPAT point of contact receives a list of Portal problems from field office security specialists, creates a work ticket for each problem, and works with TASPD staff to prioritize those work tickets and group them into batches. TASPD staff then attempt to identify the causes of the batched Portal 2.0 problems and test the proposed fixes with input from the end users (primarily security specialists and C-TPAT field office directors) to ensure the problems are corrected during 2 to 3 week intervals called "sprints." C-TPAT field office staff we met with told us that while these sprints have generally resolved the originally-identified problems, the fixes have, at times, created new problems that affected the accuracy of data and the usability of certain Portal 2.0 features. For example, security specialists have encountered error messages when trying to submit security validation reports for supervisory review and, in fixing that problem, security validation reports became inadvertently

archived, which prevented supervisory security specialists from being able to review and edit the reports.

Because of the continued Portal 2.0 problems, C-TPAT and TASPDP staff have worked together to identify root causal factors that led to the Portal 2.0 problems and are implementing actions to address those factors. For example, TASPDP staff cited unclear requirements for the Portal 2.0 system and its user needs as a factor that likely contributed to inadequate system testing and continued problems. In response, TASPDP and C-TPAT staff have begun efforts to better capture Portal 2.0 system requirements and user needs and have incorporated more consistent end user testing. Additionally, TASPDP and C-TPAT headquarters staff began having regular meetings with C-TPAT field office managers to institute a more-encompassing approach for addressing and understanding system requirements and Portal 2.0 functionality problems. As part of the root cause analysis, TASPDP staff have outlined recommended actions for addressing causal factors that led to the Portal 2.0 problems, along with the associated timeframes for completing these actions. While TASPDP and C-TPAT staff have already implemented some actions, such as establishing a new team structure, the staff stated that they will continue to work on identifying and addressing potential root causes of the Portal 2.0 problems and noted that this process will likely continue through 2017.

Issuing Standardized Guidance to Field Offices Could Better Assure Data on Security Validations Are More Consistent and Reliable

Despite the Portal 2.0 problems, C-TPAT headquarters officials and field office directors we met with told us that they are assured that required security validations are being identified and completed in a timely manner because the field offices keep records on required and completed security validations apart from data recorded in Portal 2.0. C-TPAT officials provided us with documentation illustrating the steps taken by security specialists and supervisors at the field offices to identify and complete the required security validations. Field office directors or supervisors then verify that the security validations were completed, as required, by the end of each calendar year. We reviewed this documentation and verified that field offices are tracking completed validations annually. C-TPAT headquarters staff have delegated responsibility to field office directors for ensuring that the required security validations are tracked and completed and reported to headquarters each year, but headquarters has not issued centralized guidance or standard operating procedures to be used by the field offices to ensure that they are tracking and completing the required security validations in a consistent manner. As a result, the field offices have each developed their own varied approaches for tracking required

security validations and recording those that are completed. A C-TPAT headquarters official responsible for reviewing security validation information provided by the field offices stated that there may be value in standardizing the approach field offices use to track and report on completed security validations in order to ensure the data received and reviewed by C-TPAT headquarters are more consistent and reliable. While the current validation tracking processes used by field offices do account for security validations conducted over the year, standardizing the process used by field offices to track required security validations could strengthen C-TPAT management's assurance that its field offices are identifying and completing the required security validations in a consistent and reliable manner.

Standards for Internal Control in the Federal Government related to the use of quality information state that management is to obtain relevant information from reliable internal sources on a timely basis in order to evaluate the entity's performance.¹⁹ In addition, such quality information is to flow down from management to personnel, as well as up from personnel to management, to help ensure that key program objectives are met. This upward communication also helps provide effective oversight of internal controls. The internal control standards also call for management to document responsibilities for operational processes through policies.

Developing standardized guidance for its field offices to use in tracking required security validations could further strengthen C-TPAT management's assurance that its field offices are identifying and completing the required security validations in a consistent and reliable manner.

¹⁹[GAO-14-704G](#). Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks.

CBP Cannot Determine the Extent to Which C-TPAT Members Are Receiving Benefits Because of Data Concerns

CBP Staff Have Concerns Regarding the Accuracy of C-TPAT Member Benefit Data

Since 2012, CBP has compiled data on certain events or actions it has taken regarding arriving shipments—such as examinations, holds, and processing times—for both C-TPAT and non-C-TPAT members through its C-TPAT Dashboard.²⁰ However, based on GAO’s preliminary analyses of data contained in the Dashboard, and data accuracy and reliability concerns cited by C-TPAT program officials, we concluded that CBP staff are not able to determine the extent to which C-TPAT members are receiving benefits, such as reduced likelihood of examinations of their shipments and expedited shipment processing, compared to non-members.

We conducted preliminary analyses of C-TPAT program data from the Dashboard to understand, for example, how the examination rates of C-TPAT members’ shipments compared with those of non-C-TPAT members across different modes of transportation (air, truck, vessel, and rail) for each year from fiscal year 2011 through fiscal year 2015. The results of our analyses showed that C-TPAT members’ shipments did not consistently experience lower examination and hold rates and processing times compared to non-members’ shipments across the different modes of transportation.

²⁰In 2012, C-TPAT, in collaboration with CBP’s Office of Information Technology, developed the C-TPAT Dashboard data reporting tool (Dashboard). The Dashboard is a web-based application that extracts data from various CBP sources to provide C-TPAT management with the capability to develop customized reports showing, for example, examination and hold rates and average processing times for C-TPAT member shipments and non-C-TPAT member shipments. Though the Dashboard was developed in 2012, C-TPAT officials were able to use the Dashboard to query and provide us with data dating back to fiscal year 2011.

We shared the results from our preliminary analyses with the C-TPAT Director and staff familiar with the C-TPAT Dashboard and they expressed surprise that the data did not show more consistent benefits for C-TPAT members as compared to non-C-TPAT members, and that Tier II members did not consistently receive the benefit of lower examination and hold rates or processing times as compared to Tier I members. We further discussed that the findings from our analyses ran counter to C-TPAT member benefits information published by CBP. In particular, we noted that in its *C-TPAT Program Benefits Reference Guide*, CBP asserts that entries filed by Tier III Partners are 9 times less likely to undergo a security based examination than are entries filed by non-C-TPAT members and that entries filed by Tier II Partners are about 3.5 times less likely to undergo a security examination than are those filed by non-C-TPAT members.²¹ Further, CBP's Congressional Budget Justification for Fiscal Year 2016 states that C-TPAT importers are 4 to 6 times less likely to incur a security or compliance examination than those for non-C-TPAT members.²²

Subsequent to our discussion with C-TPAT staff on the results of our preliminary analyses and the apparent discrepancy with CBP-reported benefits data, the C-TPAT Director and staff researched the data and calculations within the Dashboard further. Based on their research, the C-TPAT officials stated that there appear to be errors in the data or formulas used to compute various actions that are uploaded into the Dashboard, such as shipment examinations, holds, and processing times. For example, the C-TPAT Director stated that based on their research, they discovered errors in the data contained in the Dashboard regarding the number of CBP shipment examinations on the southwest border in 2015.

C-TPAT officials have not yet determined what accounts for the apparent accuracy and reliability issues of data contained in the Dashboard. The C-TPAT Program Director explained that the Dashboard was developed in response to a request for increased data on C-TPAT member benefits by a former C-TPAT Program Director. The current Director noted that the C-TPAT office has not regularly reviewed the data contained in the Dashboard. In addition, officials from the C-TPAT program, as well as

²¹U.S. Customs and Border Protection, *Customs-Trade Partnership Against Terrorism (C-TPAT) Program Benefits Reference Guide*, CBP Publication No. 0192-0114 (Washington, D.C.: January 2014).

²²Department of Homeland Security, *U.S. Customs and Border Protection Budget Overview, Fiscal Year 2016 Congressional Justification*.

from TASP, explained that while the Dashboard has been in place since 2012, it has functioned in a limited operational mode, with data from the Dashboard only being used internally by program management. The officials stated that the Dashboard's requirements are dated, and that new requirements need to be verified and tested. They further stated that because of competing priorities, CBP staff have not completed verification, user acceptance testing, or periodic data checks. C-TPAT officials noted, though, that C-TPAT and TASP staff are in the process of analyzing data contained in the Dashboard to finalize an action plan to correct the data concerns. It is too soon for us to assess whether this process will fully address the Dashboard accuracy and reliability issues.

Standards for Internal Control in the Federal Government state that program management should use quality information to achieve the entity's objectives.²³ Specifically, management is to obtain relevant data from reliable internal and external sources based on identified information requirements. These sources should provide data that are reasonably free from error and bias and represent what they purport to represent. Also, management should process data into quality information. Quality information is to be, among other things, appropriate, current, complete, and accurate. In addition, the SAFE Port Act requires CBP to extend benefits, which may include reduced examinations of cargo shipments, to Tier II and Tier III C-TPAT members.²⁴ As mentioned earlier, the 2014 *C-TPAT Program Benefits Reference Guide* also cites reduced examination rates for C-TPAT importers compared to non C-TPAT importers as a benefit of the program. Further, project management criteria established by the Project Management Institute state that it is necessary to establish project objectives and outline a plan of action, via a project schedule with major milestones, to obtain those objectives.²⁵

Because the data contained in the Dashboard cannot currently be relied upon, CBP is not able to determine the extent to which C-TPAT members have received benefits, such as lower examination or hold rates, or reduced processing times of their shipments when compared to non-C-TPAT members. CBP has likely relied on such questionable data since it developed the Dashboard in 2012, and, thus, cannot be assured that C-

²³ [GAO-14-704G](#).

²⁴ 6 U.S.C. §§ 965(b)(2), 966(c)(2).

²⁵ Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* – Fifth Edition, 2013.

TPAT members have consistently received the benefits that CBP has publicized.

Other C-TPAT Member Benefits Are Difficult to Quantify

Beyond shipment examination and hold rates, and processing times, CBP does not gather data on its other stated C-TPAT member benefits. There are a variety of reasons for this, including the inherent difficulty in being able to quantify certain benefits that are more qualitative in nature, such as having access to security specialists; or are difficult to meaningfully quantify across ports because of the many differences that exist in infrastructure from port to port. C-TPAT officials explained that, although these other benefits are difficult to measure, they are of value to C-TPAT members. The C-TPAT officials acknowledged that while the C-TPAT program might be able to gather and track quantifiable data on some additional benefits—such as increased mitigation of monetary penalties for C-TPAT members—given the Portal 2.0 and Dashboard data accuracy and reliability issues (as described earlier), they plan to focus first on identifying and correcting these data issues for those benefits currently tracked rather than trying to quantify and track other current member benefits.

CBP is Considering Additional C-TPAT Member Benefits and a New Metric

In addition to the C-TPAT member benefits listed earlier, CBP staff are working with trade industry partners and the COAC, to identify and explore potential new benefits, as well as a metric for quantifying potential cost savings for members.²⁶ Trade industry officials we met with generally spoke positively of the C-TPAT program and of CBP staffs' efforts in sharing information and listening to their concerns and suggestions for enhancing the program. However, some trade industry officials we met with have also expressed the desire for C-TPAT to improve and add member benefits. In response to suggestions from members of the trade community, C-TPAT staff said that they are considering some additional benefits, such as the following:

Advanced Qualified Unlading Approval (AQUA) Lane: The AQUA Lane pilot is a joint partnership between the C-TPAT program, sea carriers, and world trade associations at select U.S. ports with the goal of reducing the amount of time that the carriers must wait for releasing their

²⁶COAC advises and provides recommendations to the Secretaries of the Department of the Treasury and DHS on the commercial operations of CBP and related DHS and Treasury functions.

cargo. At these pilot ports, select C-TPAT member vessel carriers, who qualify under a set of predetermined requirements, are allowed to offload—but not release—cargo containers arriving at one of the pilot ports prior to CBP officials clearing the vessel carrier for release.²⁷ AQUA Lane was initially piloted at the ports of Oakland, California; Port Everglades, Florida; New Orleans, Louisiana; and Baltimore, Maryland. According to C-TPAT officials, the pilot has been well received by sea carriers, who have expressed interest in seeing the program expanded to other domestic sea ports. In response, CBP announced a phased expansion of the AQUA Lane program, adding six ports in September 2016, an additional 10 ports in December 2016, with final implementation to all remaining seaports to be completed in early 2017.²⁸

Trusted Trader Program: The Trusted Trader Program is a CBP-led collaborative effort being tested that aims to enhance information sharing between government agencies regarding importers' efforts to enhance supply chain security and comply with trade requirements.²⁹ As this program is expanded, one goal is to reduce redundancies in processing steps, as well as in the vetting and validation procedures of the C-TPAT and ISA programs. For example, under the Trusted Trader Program, CBP may conduct C-TPAT supply chain security and ISA trade compliance validations jointly, reducing time and resources that member companies

²⁷To receive AQUA Lane privileges, the sea carrier must: (1) be a certified member of C-TPAT (at the carrier and terminal locations), (2) be compliant with Importer Security Filing requirements, (3) be compliant with CBP agriculture requirements to include possession of all required certificates, (4) have a crewmember remain onboard until formal CBP processing, and (5) deliver all containers to a C-TPAT terminal operator.

²⁸The six ports in Phase II of the AQUA Lane Program were Los Angeles and Long Beach California; Miami, Florida; Savannah, Georgia; Newark, New Jersey; and Seattle/Tacoma, Washington. The 10 ports in Phase III of the AQUA Lane Program were Wilmington, Delaware; Jacksonville, Florida; Honolulu, Hawaii; Boston, Massachusetts; Wilmington, North Carolina; Philadelphia, Pennsylvania; San Juan, Puerto Rico; Charleston, South Carolina; Houston, Texas; and Norfolk, Virginia.

²⁹The Trusted Trader program is designed to unify the C-TPAT and ISA programs' processes in order to integrate supply chain security and trade compliance. The ISA program is a voluntary approach to trade compliance that allows interested importers to assess and monitor their own compliance with relevant laws and CBP's regulations in exchange for certain benefits. The development of the Trusted Trader Program is a coordinated effort with members of the trade community, with a goal of providing additional incentives and enhancing efficiencies of managing supply chain security and trade compliance. CBP has been working with other participating government agencies, such as the Food and Drug Administration, Department of Agriculture, Department of Commerce, United States Coast Guard, and the Transportation Security Administration to pilot the program.

must invest in these processes. However, the program has received mixed reactions from members of the trade industry with whom we met. While some members of the trade industry spoke favorably of the Trusted Trader Program, other members questioned whether the program's benefits offered sufficient incentives compared to the costs and administrative requirements.

Cost Savings Benefit Metric: CBP is in the process of reviewing a metric regarding the cost savings derived by C-TPAT members as the result of a reduced rate of shipment examinations. This metric was proposed by a C-TPAT member in the summer of 2015 and accepted by DHS consistent with the Government Performance and Results Act.³⁰ CBP began gathering data for this metric during fiscal year 2016; however, C-TPAT officials noted that they need to revisit the integrity of the supporting data that would be used in this metric as a result of the concerns we and C-TPAT officials have raised before CBP can pursue implementing such a metric.

Conclusions

CBP's risk-informed approach to supply chain security focuses on ensuring the expeditious flow of millions of cargo shipments into the United States each year, while also managing security concerns. It is critical that CBP manages the C-TPAT program in a way that enhances the security of members' global supply chains, while also providing benefits that incentivize program membership. A lack of reliable data has challenged CBP's ability to manage the C-TPAT program effectively. In particular, problems with the C-TPAT program's updated Portal 2.0 data system that began in August 2015 have impaired the ability of C-TPAT staff to identify and complete required security validations in a timely and efficient manner. While C-TPAT field offices have implemented procedures for ensuring that required security validations are identified and completed, these procedures are varied because C-TPAT headquarters has not developed standardized guidance for its field offices to follow. Taking steps to standardize C-TPAT field offices' efforts to track required security validations could strengthen C-TPAT management's assurance that its field offices are identifying and completing the required security validations in a consistent and reliable manner. Further, because the data contained in the Dashboard cannot be relied upon, CBP is not

³⁰The Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (1993), was updated by the GPRA Modernization Act of 2010, Pub. L. No. 111-352, 124 Stat. 3866 (2011).

able to determine the extent to which C-TPAT members are receiving benefits, such as lower examination or hold rates, or reduced processing times of their shipments when compared to those for non-C-TPAT members. Finally, because CBP has likely relied on such questionable data since the Dashboard was developed in 2012, it does not have reasonable assurance, consistent with federal internal control standards, that C-TPAT members have consistently received the benefits that CBP has publicized. Accurate and reliable data will also be important as CBP considers adding additional member benefits and developing a cost savings metric.

Recommendations for Executive Action

To ensure that C-TPAT program managers are provided consistent data from the C-TPAT field offices on security validations, we recommend that the Commissioner of U.S. Customs and Border Protection develop standardized guidance for the C-TPAT field offices to use in tracking and reporting information on the number of required and completed security validations.

Further, to ensure the availability of complete and accurate data for managing the C-TPAT program and establishing and maintaining reliable indicators on the extent to which C-TPAT members receive benefits, we recommend that the Commissioner of U.S. Customs and Border Protection determine the specific problems that have led to questionable data contained in the Dashboard and develop an action plan, with milestones and completion dates, for correcting the data so that the C-TPAT program can produce accurate and reliable data for measuring C-TPAT member benefits.

Agency Comments and Our Evaluation

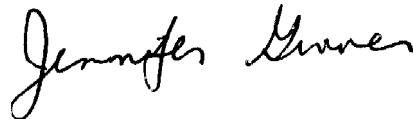
In December 2017, we requested comments on a draft of this report from DHS. In January 2017, officials from CBP provided technical comments, which we have incorporated into the report as appropriate. In addition, DHS provided an official letter for inclusion in the report, which can be seen in appendix II. In its letter, DHS stated that it concurred with our two recommendations and has begun to take actions to address them. In particular, for the first recommendation, DHS noted that the C-TPAT program manager has selected a methodology that will include uniform monthly reporting from C-TPAT field offices to the C-TPAT program manager. DHS anticipates that these efforts will be put into effect by May 2017. We will continue to monitor CBP's efforts in addressing this recommendation.

Regarding the second recommendation, DHS noted that the C-TPAT program manager has decided, in conjunction with CBP'S Office of Information Technology, to terminate the existing Dashboard reporting tool and, instead, create a new tool for providing accurate data for measuring C-TPAT member benefits by the end of June 2017. We will continue to monitor CBP's efforts in addressing this recommendation.

We are sending copies of this report to the Secretary of Homeland Security, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-7141, or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely Yours

A handwritten signature in black ink that reads "Jennifer Grover". The signature is written in a cursive, flowing style.

Jennifer Grover
Director
Homeland Security and Justice

Appendix I: Further Details on the Customs-Trade Partnership Against Terrorism (C-TPAT) Member Screening Process

This appendix provides further details on the process used to screen prospective members of the Customs-Trade Partnership Against Terrorism (C-TPAT) program.

1. **Application and eligibility:** An entity submits an application for C-TPAT membership that includes corporate information (e.g., company size and location), a supply chain security profile, and an agreement to voluntarily participate in the C-TPAT program. In completing the supply chain security profile, the entity is to conduct a comprehensive self-assessment of its supply chain security procedures or practices using the C-TPAT minimum security criteria for its specific business type, such as importer, highway carrier, or customs broker. The application is assigned to a supply chain security specialist to be reviewed to determine if the applicant meets C-TPAT eligibility requirements for its business type.¹
2. **Vetting:** Once a security specialist determines an applicant is eligible for C-TPAT membership, the security specialist is to conduct research as part of the vetting process. Vetting involves a review of the entity's compliance with Customs laws and regulations; as well as any violation history to identify information that might preclude C-TPAT membership. Once any issues are resolved to U.S. Customs and Border Protection's (CBP) satisfaction, the entity can move on to the certification stage.
3. **Certification:** After vetting, a security specialist is to conduct a detailed review of the entity's security profile, looking for any weaknesses or gaps in security procedures or practices, to determine whether minimum security criteria for that entity's business type are adequately addressed. This review is to be completed and the application approved or rejected within 90 calendar days from the date the entity submits its security profile. If the security specialist approves the security profile, the entity is certified as a C-TPAT member and is eligible to begin receiving benefits.
4. **Validation:** Once certified, a security specialist is to conduct a validation of the security measures outlined in a certified member's security profile to ensure that they are reliable, accurate, effective, and align with CBP's minimum security criteria. As provided for in the

¹As an example of C-TPAT eligibility requirements, importers must be active importers with an office in the United States or Canada, have an active U.S. importer of record identification number, and have a designated primary cargo security officer responsible for C-TPAT, among other things.

Security and Accountability for Every Port Act of 2006 (SAFE Port Act), a member's initial security validation is to be completed within 1 year of certification, to the extent practicable.² During the validation process, the assigned security specialist is to meet with the member's representatives to verify that the supply chain security measures contained in its security profile are in place as described. If the member is an importer operating a global supply chain, the security specialist is to visit the member's domestic site and at least one foreign supply chain partner's site (e.g., a manufacturer who supplies goods).³ C-TPAT management and the security specialist assigned to a member are to identify potential sites to visit based on research of the member's business history, import transportation modes, facility locations, and other factors. To initiate the security validation, the assigned security specialist is to provide the member a site visit agenda and documents to help the member prepare for the visit, such as a validation checklist. Upon completion of the security validation process, the security specialist is to prepare a final validation report to present to the member. The report may include recommendations to improve security practices, as well as any required actions the member is to take to conform to CBP's minimum security criteria. The security validation report is also to address whether the member should continue to receive program benefits; and, if an importer or exporter, whether additional benefits are warranted.

5. Annual reviews and revalidations: Once a security specialist validates a C-TPAT member's security practices, the member company is to undergo a review of its eligibility status, vetting, and certification processes on an annual basis. This involves having the member perform an annual self-assessment—essentially an update of its security profile—that provides the member with an opportunity to review, update, or change its security procedures, as needed. Security specialists are to annually certify completion of these member self-assessments. Each C-TPAT member is to undergo a security revalidation not less than once every 4 years after its initial validation, as determined by C-TPAT and in accordance with the SAFE Port Act.⁴ A security revalidation calls for a security specialist to

²6 U.S.C. § 965(a).

³In some instances, a foreign entity may have undergone a type of security validation conducted in its home country. CBP may accept this validation in lieu of conducting its own if the entity's validation was conducted by a customs administration with which CBP has a mutual recognition arrangement (MRA).

⁴6 U.S.C. § 969(2).

conduct updated document reviews and on-site visits to a member and at least one of its foreign supply chain partners to ensure continued alignment with C-TPAT's minimum security criteria.⁵

⁵CBP officials have stated that revalidations may or may not include a visit to the member's domestic site based on previous validation visit locations and assessments of risk in the supply chain.

Appendix II: Comments from the Department of Homeland Security

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



**Homeland
Security**

January 19, 2017

Jennifer Grover
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-17-84, "SUPPLY CHAIN SECURITY: Providing Guidance and Resolving Data Problems Could Improve Management of the Customs-Trade Partnership Against Terrorism (C-TPAT) Program"

Dear Ms. Grover:

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

The Department is pleased to note GAO's positive recognition of U.S. Customs and Border Protection's (CBP) achievements in maintaining a Customs-Trade Partnership Against Terrorism (C-TPAT) program that helps to secure the supply chain and protect national security, while facilitating legal trade and supporting the American economy. In particular, the draft report highlights the positive responses of industry officials with whom GAO surveyed, as the C-TPAT program strives to be a mutually beneficial partnership between CBP and the trade community.

It is important to note the benefits of the C-TPAT Program extend beyond the rate of examination and include access to the Free and Secure Trade (FAST) lanes, front of the line processing, business resumption, expedited trade processing, access to a C-TPAT Supply Chain Security Specialist, access to the Portal System, eligibility to participate in the importer self-assessment program, and penalty mitigation. Additional benefits are currently being explored through CBP's Trusted Trader pilot program. Each of the program's benefits – both current and planned – can be quantified to varying extents. More importantly, the prevention of a terrorist incident, the most compelling reason for this program's existence, can never be quantified in data or dollars.

CBP has taken many actions to improve the C-TPAT portal. For example, CBP has culled data from the Automated Targeting System, along with reports on Non-Intrusive Inspection machine operations as it pertains to the rail environment, which provides accurate rates of examination experienced by C-TPAT members in comparison to trade members that are not in the program. Moving forward, the program will be building upon this work to assure that CBP can efficiently and precisely assess the implementation of the reduced rate of examination benefit provided to C-TPAT members.

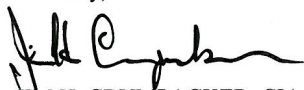
In addition, a newly contracted development team officially assumed programming responsibility in September 2016. The team immediately implemented a new development strategy and a rigorous testing regimen to prevent flawed deployments. Also, since December 2016, numerous updates have been made to the C-TPAT Portal, to include updated Importer and Exporter entity security profile questions, international harmonization, and verification of status between partners.

The Department is committed to continuing to strengthen cargo security throughout the international supply chain by working closely with importers, carriers, consolidators, licensed customs brokers, and manufacturers.

The draft report contained two recommendations with which the Department concurs. Attached find our detailed response to each recommendation.

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

Sincerely,



J. H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: DHS Management Response to Recommendations
Contained in GAO-17-84**

GAO recommended that the Commissioner of U.S. Customs and Border Protection (CBP):

Recommendation 1: Develop standardized guidance for the field offices to use in tracking and reporting on the number of required and completed security validations.

Response: Concur. The C-TPAT program manager assessed the efficiency and clarity of the manual tracking methods of the seven field offices. After this comparative review, the program manager selected a methodology which has been structured into the 2017 validation work plan. This methodology will include uniform monthly reporting to the program director, so that appropriate adjustments, if necessary, can be made throughout the year. Estimated Completion Date (ECD): May 31, 2017.

Recommendation 2: Determine the specific problems that have led to questionable Dashboard data and develop an action plan, with milestones and completion dates, for correcting the Dashboard data so that the C-TPAT program can produce accurate and reliable data for measuring C-TPAT members' benefits.

Response: Concur. In November 2016, the C-TPAT program manager began discussions to evaluate the nature of the program's need for an accurate reporting mechanism. The program manager, in conjunction with CBP's Office of Information and Technology, determined that the existing C-TPAT Dashboard should be terminated. Tailoring existing data logic, the program manager produced reports from the Automated Targeting System to obtain accurate data concerning rate of examination. The program manager also assessed Non-Intrusive Inspection machine operations concerning the rail environment in conjunction with the data in December 2016. The program manager will continue to leverage this work to create an interface that will allow the program to assess the efficacy, to the extent possible, of the rate of examination. The program's plan will include various presentations and a substantive testing period, as to best ensure that the program can rely on what is produced. ECD: June 30, 2017.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer Grover, (202) 512-7141 or groverj@gao.gov

Staff Acknowledgments

In addition to the contact above, Christopher Conrad (Assistant Director), Adam Couvillion (Analyst-in-Charge), David Alexander, Christine Broderick, Charles Bausell, Dominick Dale, Dorian Dunbar, Tyler Mountjoy, Heidi Nielson, Nina Thomas-Diggs, and Eric Winter all made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

E-mail: fraudnet@gao.gov

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.