S. Hrg. 109–186

THE CONTAINER SECURITY INITIATIVE AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM: SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?

HEARING

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 26, 2005

Printed for the use of the Committee on Homeland Security
and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

21–825 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Chief Counsel*
TRINA D. TYRER, *Chief Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

NORM COLEMAN, Minnesota, *Chairman*

TED STEVENS, Alaska
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

RAYMOND V. SHEPHERD, III, *Staff Director and Chief Counsel*
BRIAN M. WHITE, *Professional Staff Member*
ELISE J. BEAN, *Minority Staff Director and Chief Counsel*
LAURA E. STUBER, *Minority Counsel*
MARY D. ROBERTSON, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Coleman	1
Senator Levin	5
Senator Collins	7
Senator Akaka	9
Senator Lautenberg	10
Senator Carper	33

WITNESSES

THURSDAY, MAY 26, 2005

Hon. Robert C. Bonner, Commissioner, Customs and Border Protection, U.S. Department of Homeland Security	12
Richard M. Stana, Director, Homeland Security and Justice Issues, U.S. Government accountability Office	37
Stephan E. Flynn, Commander, U.S. Coast Guard (Ret.), Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations, New York, New York	40
C. Stewart Verdery, Jr., Principal, Mehlman Vogel Castagnetti, Inc., Adjunct Fellow, Center for Strategic and International Studies, and Former Assistant Secretary of Border and Transportation Security Policy, U.S. Department of Homeland Security	43

ALPHABETICAL LIST OF WITNESSES

Bonner, Hon. Robert C.:	
Testimony	12
Prepared statement with attachments	53
Flynn, Stephen E.:	
Testimony	40
Prepared statement	94
Stana, Richard M.:	
Testimony	37
Prepared statement	66
Verdery, C. Stewart, Jr.:	
Testimony	43
Prepared statement	102

EXHIBITS

1. *High-Risk Shipments and Exams Conducted at Selected CSI Ports 2004—CSI Ports: Hong Kong, Yokohama, and Le Havre,* chart prepared by the Permanent Subcommittee on Investigations	108
2. *High-Risk Shipments and Exams Conducted at Selected CSI Ports 2004—CSI Ports: Durban, Gothenburg, and Rotterdam,* chart prepared by the Permanent Subcommittee on Investigations	109
3. *Status of Validating C-TPAT Members as of April 15, 2005 (Not Validated/Validated),* chart prepared by the Permanent Subcommittee on Investigations	110
4. *C-TPAT Membership Process,* chart prepared by the Permanent Subcommittee on Investigations	111
5. *Status of Validating C-TPAT Members as of April 15, 2005 (Non-importers/Importers),* chart prepared by the Permanent Subcommittee on Investigations	112
6. Photograph of the Port of Hong Kong	113

Page

7. Photograph of Heimann Mobile x-ray at the Port of Felixstowe, England .. 114
8. U.S. Government Accountability Office (GAO) Report to Congressional Requesters, *CARGO SECURITY—Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security,* March 2005, GAO-05-404 115
9. U.S. Government Accountability Office (GAO) Report to Congressional Requesters, *CONTAINER SECURITY—A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* April 2005, GAO-05-557 154
10. Responses to supplemental questions for the record submitted to Robert C. Bonner, Commissioner, U. S. Customs and Border Protection, Department of Homeland Security 204
11. Responses to supplemental questions for the record submitted to Richard M. Stana, Director, Homeland Security & Justice Team, Government Accountability Office 215
12. Photograph and x-ray image taken at a Michigan port of a container carrying Canadian trash 217

THE CONTAINER SECURITY INITIATIVE AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM: SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?

THURSDAY, MAY 26, 2005

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:32 a.m., in room SD–106, Dirksen Senate Office Building, Hon. Norm Coleman, Chairman of the Subcommittee, presiding.

Present: Senators Coleman, Collins, Levin, Akaka, Carper, and Lautenberg.

Staff Present: Raymond V. Shepherd, III, Staff Director and Chief Counsel; Mary D. Robertson, Chief Clerk; Brian M. White, Professional Staff Member; Leland Erickson, Counsel; Mark Nelson, Counsel; Katherine Russell, Detailee (FBI); Jeffrey James, Detailee (IRS); Richard Fahy, Detailee (ICE); Elise J. Bean, Staff Director and Chief Counsel to the Minority; Laura E.Stuber, Counsel to the Minority; Eric J. Diamant, Detailee (GAO); Merril Springer, Intern; and Adam Wallwork, Intern.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. This hearing of the Permanent Subcommittee on Investigations is called to order. Good morning and thank you all for being here today.

Today's hearing presents the first opportunity for this Subcommittee to examine key homeland security programs under the recently restructured full Committee on Homeland Security and Governmental Affairs. I look forward to working collaboratively with the full Committee and holding several additional oversight hearings on homeland security in the future.

After September 11, unfairly or not, Customs and Border Protection (CBP) was thrust onto the front lines of our war on terrorism. CBP was placed in the untenable position of having to transform itself overnight—from an agency focused on interdicting guns, drugs, and money—to the agency chiefly responsible for protecting us against a chemical, biological, radiological, or nuclear attack. Commissioner, I want to thank you for your efforts to date in leading this transformation.

Today's hearing will focus on the Federal Government's efforts to secure maritime commerce and the global supply chain. In early 2002, U.S. Customs and Border Protection launched both the Container Security Initiative (CSI), and the Customs-Trade Partnership Against Terrorism (C–TPAT), to address the threat of terrorism and the security of the global supply chain. These programs were, and still are, the right concepts for security in our new threat environment. Under the leadership of Commissioner Bonner, CBP aggressively implemented these programs, rather than endlessly debate the details here in Washington. That accomplishment alone is worth applauding.

However, these programs have been in existence for over 3 years and it is time to start asking some tough questions and identifying how we can improve upon these promising concepts. While I believe these programs are indeed the right concepts, our oversight investigation into these programs has revealed significant shortcomings that we will address here today. In concert with our efforts, the Government Accountability Office (GAO), conducted two extensive audits of these programs. These reports reveal some significant problems and outline the substantial work that is required to transition these promising initiatives into effective and sustainable programs.

As Secretary Chertoff stated at a full Committee budget hearing in March, "the worst thing would be this: To have a program for reliable cargo that was insufficiently robust so that people could sneak in and use it as a Trojan Horse. That would be the worst of all worlds." Rest assured that PSI will conduct the necessary sustained oversight to strengthen these programs and ensure that they are not used as a Trojan Horse by those whose very raison d'etre is to destroy us.

If there was one thing my colleague, Senator Kerry, and President Bush agreed on in their debates this past fall, it was the threat of nuclear terrorism. When both were asked about the "single most serious threat to the national security of the United States, Senator Kerry responded, nuclear proliferation, nuclear proliferation." In response, President Bush concurred and told the audience, "I agree with my opponent that the biggest threat facing this country is weapons of mass destruction in the hands of a terrorist network."

Senator Kerry and President Bush agreed because the stakes are so very high. In a recent estimate, a 10 to 20 kiloton nuclear weapon detonated in a major seaport would kill between 50,000 to one million people and result in direct property damage of $50 to $500 billion, losses due to trade disruption of $100 billion to $200 billion, and indirect costs of $300 billion to $1.2 trillion. This is unfathomable and demonstrates why these programs are essential to homeland security.

Recently, Director Robert Mueller, ominously assessed the terrorist threat at the annual Global Intelligence Briefing by stating he is concerned "with the growing body of sensitive reporting that continues to show al Qaeda's clear intention to obtain and ultimately use some form of chemical, biological, radiological, nuclear, or high-energy explosives in attacks against America."

Many terrorism experts believe that maritime container shipping may serve as an ideal platform to deliver these weapons to the United States. In fact, we recently saw that containers may also serve as ideal platforms to transport potential terrorists into the United States. This was demonstrated on January 15 and again on April 2 this year, when upwards of 30 Chinese immigrants were found emerging from containers arriving at the Port of Los Angeles. I know that the Chair, Senator Collins, was surveying that port and is very familiar with the situation. The individuals were actually not seen sneaking out of a container by the cameras, rather by an observant crane operator. The Subcommittee's concern is that smuggled immigrants could include members of terrorist organizations and/or that the container could have contained a weapon of mass destruction.

The Customs-Trade Partnership Against Terrorism, or C–TPAT, attempts to secure the flow of goods bound for the United States by developing voluntary partnerships with the trade community. C–TPAT members—primarily importers—commit to improving the security of their supply chain and provide CBP with their supply chain security profiles for review. In exchange for this commitment, CBP provides C–TPAT members benefits to include upwards of seven times fewer inspection of their cargo at U.S. borders.

Our concerns with C–TPAT include, one, these substantial benefits, including fewer inspections, that are provided to importers before a thorough review or validation of their supply chain security profiles, and two, of those validations that occur, the process lacks what I would call rigor or independence. To me, a validation is an independent physical audit of the supply chain security plan provided to CBP. However, CBP views a validation as an opportunity to "share best practices" and explicitly states that "validations are not audits."

Furthermore, of the 2,676 certified C–TPAT importers receiving reduced inspections, only 6 percent, 179, have been validated. Hence, 94 percent of the C–TPAT importers currently receiving seven times fewer inspections have not had their supply chain security personally validated by a CBP officer. This is simply unacceptable.

The Container Security Initiative (CSI) was implemented to enable CBP to target high-risk containers for inspection at overseas ports prior to their departure for U.S. ports. Currently operating in 36 foreign ports, this program is based on the concept of "pushing out our borders." While this concept is laudable and it is a good concept, a review of CBP data by this Subcommittee and GAO raises significant concerns.

Many CSI ports are unable to inspect the quantity of containers necessary to significantly improve security. Our Subcommittee has identified some CSI reports that routinely "waive" the inspection of high-risk containers, despite requests by CSI personnel for an inspection. As a result, numerous high-risk containers are not subjected to an examination overseas, thereby undermining the primary objective and purpose of CSI.

More specifically, CBP inspects approximately one-third of 1 percent of the total number of containers headed for U.S. shores from CSI ports. Equipment such as nuclear detection devices and non-

intrusive inspection machines used for overseas inspections are untested and are of unknown quality. And CBP is unable to compare the performance of one CSI port to another.

And finally, Customs identified 1.95 percent of containers transiting through CSI ports in 2004 as high-risk, and that is not a bad thing. However, of those containers deemed high-risk, only 17.5 percent are inspected overseas.

Let me make the record clear. We have had a lot of discussion about numbers. CBP asserts that 90 percent of high-risk containers are inspected abroad, and when GAO states that 72 percent of high-risk containers are inspected abroad, they are referring to high-risk containers referred for inspection. When I state that only 17.5 percent of high-risk containers are inspected abroad, I am referring to all containers designated high-risk by CBP. So you have, and there is a chart showing this,[1] a number of containers designated high-risk, but then a smaller percentage which are designated for inspection, and I believe at least domestically here that we inspect all high-risk containers. And yet abroad, I think our figure of 17.5 percent is the valid figure.

While these findings are troubling, Customs has already moved aggressively to improve these programs by fulfilling the recommendations of the GAO audits. These changes are encouraging and are worth highlighting. I look forward to Commissioner Bonner's discussion of these substantial modifications. However, based on our oversight, I believe much work remains for Customs to build more robust and effective security programs—in partnership with industry—to confront the very real terrorist threat. This partnership will entail a transformation of the trade community, where security becomes embedded in the global supply chain. Instead of security being a cost of doing business, security needs to become a way of doing business.

I want to take this opportunity to thank Ranking Member Levin, Chairman Collins, Senator Lieberman, and Representative Dingell for their support and interest in this important subject. Securing our Nation's borders and ports demands a bipartisan and bicameral approach. I would also like to thank Richard Stana, of the GAO, and his outstanding team of Stephen Caldwell, Deena Richart, and Kathryn Godfrey for producing two insightful reports that will contribute to improving our homeland security.

I would like to welcome and thank the Commissioner of U.S. Customs and Border Protection, Commissioner Bonner, the Director of Homeland Security and Justice Team at GAO. Richard Stana, Commander Steven Flynn of the Council on Foreign Relations, and Stewart Verdery, the former Department of Homeland Security Assistant Secretary for Border and Transportation Security for appearing before this Subcommittee today. I look forward to their testimony and an engaging hearing.

With that, I would like to recognize my Ranking Member, Senator Levin.

---

[1] See Exhibits No. 1 and 2 which appears in the Appendix on pages 108 and 109 respectively.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you very much, Mr. Chairman. I appreciate your effort, your energy, your commitment on a very difficult subject. It is an important security issue that we are addressing here this morning and the Chairman's leadership in this effort is essential and I commend you for it.

I also want to commend our other colleagues, as you have, including Congressman John Dingell, the dean of the House, for his ongoing interest in this issue and for the major contributions that he has made to the investigation.

On September 30, 2004, President Bush said "the biggest threat facing this country is weapons of mass destruction in the hands of a terrorist network." On February 16, 2005, Porter Goss, Director of CIA, or Central Intelligence, told the Senate, "It may be only a matter of time before al Qaeda or another group attempts to use chemical, biological, radiological, or nuclear weapons." In 1998, Osama bin Laden declared that acquiring chemical or nuclear weapons "is a religious duty."

These types of statements show that blocking avenues that could be used to smuggle weapons of mass destruction into this country is of utmost importance to our security. Today's hearing focuses on one of those avenues: The 23 million containers that enter the United States each year.

The Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT), are two programs designed by Customs as part of what it has called a multi-layered strategy to detect and prevent weapons from entering the United States through containers. The two reports being released today by the Government Accountability Office (GAO), have identified deficiencies in both programs and are the focus of today's hearing.

Container security has special significance to me because each year, over 3 million containers cross the Michigan-Canadian border, 3 million containers a year. Many of these containers carry municipal solid waste from Canada and enter Michigan by truck at three ports: Port Huron, Detroit, and Sault Ste. Marie. Each month, in one of those ports, Port Huron alone, approximately 7,000 to 8,000 containers of Canadian waste enter Michigan across that border.

Leaving aside the issue of why our Canadian neighbors are sending so much trash to my home State of Michigan each day, key question is whether our Customs personnel have the technology and resources necessary to inspect those containers and ensure that they are not carrying weapons of mass destruction into our country.

One key type of detection equipment used to screen containers for security purposes uses X-rays to examine their contents. But X-rays of trash containers are usually unreadable—the trash is so dense and variable, that it is impossible to identify anomalies, such as weapons or other contraband. This photograph taken at a Michigan port of a container carrying Canadian trash illustrates the problem.[1] Anything could be stashed in the middle of one of these

[1] See Exhibit No. 12 which appears in the Appendix on page 217.

trash containers, and our border personnel would have no way of detecting anomalies in the picture, and that is what they look for, anomalies. In trash, everything is anomalous. It is the definition of trash.

The effectiveness of Customs detection equipment when it comes to trash containers is an issue that I have raised before with the Department of Homeland Security and other agencies and I raise it again today. The bottom line is that if we are relying on this equipment to detect WMD or other contraband in containers filled with trash, we are putting our faith in a faulty and limited system. We need to address that problem.

The GAO reports raise a number of other very troubling container security issues that need to be addressed, and just a few of them, I will highlight here.

First, inspection failures at foreign ports. The Chairman has addressed this issue and I will quickly summarize. One key problem identified in the GAO reports is the ongoing failure of the CSI program to convince foreign governments to inspect containers identified by U.S. personnel as high-risk cargo. I want to emphasize what the Chairman said. This is cargo we have identified as high-risk cargo. Now, the GAO found that 28 percent of the containers referred by U.S. personnel to a host government were not inspected. Maybe someone wants to argue over the percentage. I will stay with the GAO. But whether it is 10 percent, 20 percent, or 28 percent, every one of those containers that are high-risk containers identified by us should be inspected.

One out of four containers, according to the GAO numbers, identified by U.S. personnel as high-risk cargo were not inspected. If these high-risk containers are not being inspected overseas, then why are we letting them into the United States?

Another issue is overseas personnel costs. Another issue of concern involves CSI staffing levels overseas, and whether we are spending a needless amount of money to maintain U.S. personnel at foreign ports. We obviously want U.S. personnel at foreign ports, but the idea that we are paying an average cost of $430,000 annually, per year, to keep each American overseas is amazingly high. It is a figure which is incredibly high to me, and the latest figures from Customs indicate there are currently 114 Customs employees overseas at 36 ports.

Now, it is helpful to have that staff working directly with host nations, and I am all for it. We ought to do it at a much more reasonable cost than that, but I am all for it. But typically, only one or two CSI team members deal directly with the host government's customs officials, while others work primarily at computers, analyzing data. The question is whether it is cost effective to place an entire CSI team at a port when only one or two individuals are personally interacting with foreign government personnel.

Then we have the C–TPAT program. We have an automatic reduction in containers' scores because of that Partnership Against Terrorism. The reduction in the score is automatic and the question is whether or not it should be, where you automatically ease inspection standards for each shipper that signs up for the program. Right now, as soon as the shipper files the application to become a C–TPAT member, Customs immediately reduces the shipper's

Automatic Targeting System (ATS) score by a sizeable amount of points, without any verification that a reduced score is appropriate.

A sizeable, automatic point reduction is of concern because it may be enough to move a shipper from a high-risk category to a medium- or even low-risk category, reducing the chance that the shipper's containers will be inspected, even if the shipper hasn't yet met the program's minimum security requirements, and that is the issue. C–TPAT members shouldn't get the benefits of the program's just for signing up. The shipper should also have to show that it is meeting the program's security requirements to get the benefits.

Customs carried on the approval at a fairly slow pace, and validating those plans has also been fairly slow. So after 3 years, Customs approved only about 50 percent of the security plans submitted by C–TPAT members and rejected about 20 percent. Of the approved plans, Customs has actually validated compliance for only about 10 percent, which means that almost 90 percent of the firms that are given reduced Customs scrutiny have never undergone a validation process showing that they are entitled to the reduced scrutiny. That is a large validation gap that invites abuse and we ought to try to correct it. It may be an appropriations issue, I am not sure.

Finally, GAO has determined that DHS has no specified minimum technical requirements for the inspection equipment being developed and used at CSI ports and we need those standards in order to know whether the equipment being purchased is doing the job that needs to be done.

It is an enormous problem, this container security issue which the Committee is addressing today. It is going to require an enormous effort to address, but again, I commend our Chairman for his leadership in addressing these gaps and addressing these problems. He is doing it for exactly the right reason, which is the security of this Nation. We want to be as positive as we possibly can be to give the assistance to Customs that they need to carry out these programs efficiently and effectively.

Senator COLEMAN. Thank you, Senator Levin. I think it is interesting to note that Senator Levin, myself, and the Chairman all have States that are border States, and so these issues are particularly important.

It is always an honor to have Chairman Collins here. This has really been her issue. She has personally vested time and energy in it. She has put it on the radar screen. She has been out to various ports, surveying the situation there, and so I just want to publicly thank her for her deep concern and leadership in raising these questions, and hopefully the work of the Subcommittee will assist her in her efforts to ensure greater security and greater safety for all our ports and borders. So with that, Chairman Collins.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. Thank you very much, Mr. Chairman. Let me commend you for your efforts to assess and improve the security of our vital maritime industry.

You are correct that this issue is of great personal interest to me. I have long been concerned and convinced that our ports are one of our, if not the greatest, vulnerability that we have, and your

hearing builds very well on previous oversight hearings that we have held at the full Committee.

Coming from a State with the largest port by tonnage in New England, I am keenly aware of the importance of our seaports to our national economy. Ninety-five percent of U.S. trade, both imports and exports, moves through our seaports, and in the year 2004, the value of these imports alone exceeded $600 billion.

I also understand the link between maritime security and our national security. In my judgment, based on the work that we have done and supplemented by the excellent work of this Subcommittee, the weakest link in maritime security is the cargo container. It used to be when I would see a giant cargo ship come into a port, I viewed it as a marvel of the global economy. Now, I worry that one of those containers may include the makings of a dirty bomb, a group of terrorists, or even a nuclear weapon.

In 2004, nearly 27,000 of these potential Trojan Horses entered our country each day through our seaports. That amounts to roughly 9.7 million containers in that year. We know that most of the inbound containers are transporting legitimate goods—TV sets, sneakers, or toys. But we also know that smugglers for years have exploited the vulnerabilities of our container system to smuggle in contraband, such as drugs, illegal aliens, and other illegitimate commerce.

Given the current technology and the sheer volume of traffic, we simply cannot inspect every container without bringing trade to a standstill. We cannot follow every container through its global journey, nor can we track every container and every piece of cargo along the roads, rails, and airways that bring them to ports. No one nation can secure the international supply chain.

The two programs we examine today are designed to make securing the supply chain exactly what it should be, a shared responsibility, a shared partnership between the public and private sectors, a shared responsibility among nations.

While these programs are extremely well conceived, their level of success can only be described as modest. A substantial majority of our ports worldwide are not part of the CSI program. The overwhelming majority of private sector entities have not enrolled in C–TPAT. Terrorists are nothing if not opportunistic. These gaps in security may well be too wide to ignore.

Equally troubling, however, are the indications that the CSI and C–TPAT agreements in place are not as strong in practice as they appear to be on paper, and both of my colleagues already outlined some of the GAO's findings in this regard and we will hear from the GAO later today, so I won't repeat it here.

We should, however, recognize the fact that Customs and Border Protection was compelled to roll out these two programs very quickly during a time of great stress and uncertainty. Given the urgent need to take action against terrorism following September 11, it is understandable that these programs began with what is frequently called the implement and amend approach. In other words, get it started and fix the problems as they come up.

We must ensure, however, that the problems are, indeed, identified and fixed. The consequences of failing to do so could be staggering. The West Coast dock labor dispute in the fall of 2002 cost

our economy an estimated $1 billion for each of the 10 days that it lasted. It not only brought the affected ports to a halt, but it also harmed businesses throughout this country and among our international trading partners. And that astonishing amount of economic damage was the result of an event that was both peaceful and anticipated.

Just think what a deliberate attack on one of our large ports, or even a small port, could do to our economy. It would bring it to a standstill. It would result in all seaports being closed down temporarily, and obviously, it could cause a significant loss of life.

The use of the Trojan Horse analogy is apt. Earlier this year, as the Chairman indicated, I toured the Ports of Los Angeles and Long Beach. The size of these facilities and the amount of activity is just extraordinary to behold. But so, too, are the risks and the vulnerabilities they offer for terrorists to exploit.

I saw from the air from a Coast Guard helicopter the enormous number of containers being unloaded from ships in these two ports. By coincidence, as the Chairman mentioned, my visit came immediately before 32 Chinese nationals were smuggled into the Port of Los Angeles on two cargo containers. Fortunately, that Trojan Horse held people seeking a better way of life, not terrorists seeking to destroy our way of life.

They were caught, but what is particularly disturbing about this case is they were not caught due to any security initiative or the technology or extensive television network surveillance cameras that were in place, but rather, as the Chairman indicated, by an alert crane operator. It is also troubling that the same kind of incident happened a second time just a few months later.

We cannot continue to rely on luck or even alert crane operators to provide for the security of our seaports, our Nation, and our people.

Mr. Chairman, I look forward to hearing the testimony today.

Senator COLEMAN. Chairman Collins, I again want to thank you for your leadership on this important issue.

Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I am glad to join you in this hearing and I thank you for convening this hearing on the Container Security Initiative and the Customs-Trade Partnership Against Terrorism. These programs represent critical layers in the protection of American cargo and ports.

Cargo security is especially important to my State of Hawaii because, as I noted in many previous hearings, Hawaii receives 98 percent of the goods it imports via the sea. An interruption in sea commerce could have a staggering impact on the daily lives of the people in Hawaii.

Last week, Department of Homeland Security Secretary Chertoff stated that we need to create a world that is banded together with "worldwide security envelopes," which he described as secure environments through which people and cargo can move rapidly, efficiently, and safely. Programs such as CSI and C–TPAT, which use voluntarily submitted information to focus scarce screening re-

sources on high-risk shippers and cargo should be the cornerstones of Secretary Chertoff's vision.

It is important not only to examine whether these programs function well, but how they will fit into Secretary Chertoff's vision of a worldwide security envelope. I have yet to see details that convince me that DHS has executed the planning necessary to achieve such a coordinated global effort.

Unfortunately, there is only minimal coordination of international programs across the Department. For example, there are Immigration and Customs Enforcement, ICE, agents investigating illegal customs activities in countries that have CSI ports, and yet, often the Customs and Border Protection and ICE teams—can you imagine this—do not talk to each other.

CSI teams are scrubbing data daily, looking for anomalies relating to weapons of mass destruction, but we also must be concerned about drug smuggling, human trafficking, counterfeit goods, and invasive species. We need to ensure that our international partnerships are not program specific.

DHS's Office of International Affairs could play a critical role in coordinating operations abroad of the various entities within the Department. We need effective coordination to ensure that our various security programs are integrated and are mutually reinforcing.

I look forward to the testimony of our witnesses, and thank you so much, Mr. Chairman.

Senator COLEMAN. Thank you, Senator Akaka. Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thanks, Mr. Chairman, for holding this hearing. We have a duty in Congress to step back every once in a while and oversee how things are going. This is such an opportunity.

I concur with your comments, Mr. Chairman, about the Chairman of the entire Committee. She has been very much interested and diligent about homeland security issues, so it is a welcome addition to the dialogue here that Chairman Collins is with us.

In this case, I am afraid that the report card is one that will not make anyone particularly proud. The Administration has failed on port security. I'm concerned that if we review every program at DHS with the zeal that this Subcommittee shows here today, we might find even more frightening results.

It has been almost 4 years since September 11 and we still inspect only 5.5 percent of all containers coming into the United States. Two programs, the Container Security Initiative and the Customs-Trade Partnership Against Terrorism, are aimed at detecting terrorist weapons brought to our country. But CSI has resulted in inspections of only 17.5 percent of high-risk cargo.

The Customs and Border Protection may claim that they can only ask foreign countries to inspect for WMDs, but terrorists ship things other than weapons, too, like drugs, which are sold to pay for terrorist operations, and we rely on other nations to perform these inspections. We don't have standards for the equipment that they use to inspect. We don't even oversee some of these foreign in-

spections. In some cases, DHS personnel in the CSI program are stationed an hour away from where the actual loading takes place.

There are big problems with the CSI program, as I expect our witnesses will discuss in more detail. The bottom line, however is that the Federal Government has not been doing enough to protect our citizens from container-borne threats.

As for the C–TPAT program, it is alarming to me that after September 11, that the Administration would fashion a voluntary homeland security program to try and improve supply chains. If a voluntary program were all that was needed, then the industry could have done that on its own. If September 11 taught us anything, it should be the government has a duty to protect its citizens from terrorism, not simply rely on companies to upgrade security at isolated parts of a worldwide logistics system.

We saw that very sharply in our inspection of cargo at the airports—the baggage screenage. The private sector was doing it as a business and doing it very poorly. I am pleased to say that I have seen marked improvements in those inspection routines. If the Administration knows what security measures should be taken to improve security of our logistics system, they should require them, not make them, optional.

And finally, the Port Security Grant Program is now administered by the Office of Domestic Preparedness. Last September, the Administration announced a round of grants to help secure our ports. But those resources were not targeted to the ports that are most at risk, and it is a subject that I have discussed fairly frequently about security grants in general. Some of the grants went to facilities in Oklahoma, Indiana, and Kentucky, hardly the front lines of the war on terror, certainly not with the port presence that we have in the States that are represented here.

I think it is just common sense that Port Security Grants should be based on risk, not politics. And I know that the Inspector General has agreed with my position. We cannot afford to play politics with port security. The consequences of failure are simply too great.

Some 20 million people live near the New York-New Jersey port facilities, which are vulnerable to terrorist attacks. Hazardous materials move in and out of the port through pipelines and over roads and freight rail lines, and Newark Liberty International Airport is within a mile of the harbor or the port. So it is easy to imagine what is at stake for my State and the Nation if our port is attacked.

I am upset with the failures of the Administration on port security and I hope these hearings this day will help illuminate the dangerous lapses and loopholes that leave our citizens at risk. I hope these hearings help us find solutions for moving forward. Thank you, Mr. Chairman.

Senator COLEMAN. Thank you, Senator Lautenberg.

I would now like to call our first witness for today's hearing. It is my pleasure to welcome the Hon. Robert C. Bonner, Commissioner of U.S. Customs and Border Protection for the Department of Homeland Security.

Commissioner Bonner, I appreciate your attendance at today's hearing and look forward to your testimony regarding CBP's efforts

to secure maritime trade and the global supply chain, and let me say up front, we recognize the enormity of the task. I believe there are over 9 million eight-by-eight cargo containers that enter this country annually, and so we are looking at needles in a very big haystack. I also want to publicly thank you for your efforts to date.

We do recognize that strides have been made, tremendous improvements have been made. But certainly the purpose of oversight is to look at what we have and say, how do we make it better? The stakes are simply so high here, they are so high that, clearly, this is the kind of oversight that is needed.

Before we begin, pursuant to Rule 6, all witnesses before the Subcommittee are required to be sworn in. I would ask you to please stand and raise your right hand.

Do you swear that the testimony you are about to give before the Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BONNER. I do.

Senator COLEMAN. We will be using a timing system today. I think the oral testimony should be no more than 10 minutes. When you see the amber light come on, come to a conclusion. But your entire testimony will be entered into the record as a whole.

With that, Commissioner, please proceed.

TESTIMONY OF HON. ROBERT C. BONNER,[1] COMMISSIONER, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BONNER. I appreciate that, Mr. Chairman. I appreciate the kind words, and Senator Levin, Chairman Collins. I am very pleased to appear before the Subcommittee, Mr. Chairman, today to have this opportunity to discuss two very important initiatives of Customs and Border Protection and these are the Container Security Initiative and the Customs-Trade Partnership Against Terrorism, or C–TPAT. And I want to thank the Members of the Subcommittee for your support of CBP and the work that it does every day to help protect America and keep it safe, and by that, I mean the help that this Committee, the Subcommittee has given us to help secure our borders and our ports.

I might also say, Mr. Chairman, that the GAO and this Subcommittee and the staff of the Subcommittee have offered over the course of time some very valuable suggestions to us and recommendations with respect to both CSI and C–TPAT, and I can tell you that we appreciate the interest and oversight, and we also have taken many of these suggestions and recommendations to heart because we have implemented a good many of them.

These initiatives that I want to talk about a bit this morning, as you know, seek to add security to our country, but to do so without choking off the flow of legitimate trade that is so important to our economy.

I would say one of the realizations that I had, and I am sure many people did on the morning of September 11, was that on that morning, the priority mission of U.S. Customs, now Customs and Border Protection, became national security. The mission became

[1] The prepared statement of Mr. Bonner appears in the Appendix on page 53.

nothing short of doing everything that we could responsibly with the resources we have to prevent terrorists and terrorist weapons from getting into our country.

But I will also say, having been there, that there was another realization that came to me the following day, on September 12, 2001, and that is as important as it is that we increase our security and make it more difficult for al Qaeda and al Qaeda-associated terrorist organizations to be able to attack America and to get into this country or to get weapons into this country, we had to do that without shutting down our economy. On the morning of September 11, U.S. Customs went to the highest security-level alert that existed at that time, short of actually just shutting down the ports of entry into our country.

And the result as, by the next day, September 12, we had virtually shut down our border. The wait times at the Ambassador Bridge that comes from Ontario over to Detroit, the bridges into Buffalo from Canada, they literally froze up. We went from wait times on September 10 that averaged about 10 minutes to 12 hours by September 12 and September 13.

And so it was important that we figured out, as best we could and as quickly as we could, how we did the security in a way that didn't shut down our economy in the process, because I can tell you, by the 13th and 14th of September, as a result of the actions that we took, companies, many companies that relied on just-in-time deliveries in the United States were ready to shut down their plants. In fact, a few plants of the major automobile manufacturers did shut down on September 14.

So we have needed, as we have looked at this issue, to figure out ways that we could accomplish essentially what I would describe as twin goals: The goals of securing our country in a way that does not shut down the flow of legitimate trade and damage our economy. And those twin goals, and I have described them many times, are part and parcel of CBP's strategy of a smart border and an extended border strategy, one that pushes our zone of security out beyond our borders so that we know what is headed our way before it arrives here at our ports and so that our borders are our last line of defense, not our first line of defense. And when I say our borders here, I mean all of our ports, official ports of entry into the United States, all the official crossing points.

Our strategy, by the way, that we put together and we have implemented is essentially based upon four interrelated and interlocking initiatives. It is no one initiative. This is a layered approach that we have taken to increase significantly the security of maritime cargo and all cargo moving into the United States.

But it is built upon four key initiatives, and the first is the 24-hour and Trade Act rules, and these were rules and regulations we put into place requiring advance electronic information, initially on all ocean-going sea containers 24 hours before they were shipped to the United States, and now on all cargo shipped to the United States.

The second initiative was building and developing the Automated Targeting System that is our risk targeting system at CBP's National Targeting Center that uses targeting rules that are based upon strategic intelligence and anomaly analysis to assess for risk

of terrorism every single cargo shipment that heads to the United States before it arrives. And in the case of sea cargo containers, before it even leaves foreign seaports to the United States.

The third is the Container Security Initiative, and that, of course, is our partnership with governments, other governments of the world to screen high-risk containers before they are loaded on board vessels for the United States. To implement CSI, we have entered into CSI agreements with over 23 countries and we have implemented, that is made operational CSI at 36 of the largest foreign seaports of the world, seaports that include everything from Rotterdam to Singapore to, recently, Shanghai.

Now, these didn't all start at once. They started with one port. You have to start someplace. That was the Port of Rotterdam, by the way, as a result of an agreement with the Dutch, with the Netherlands, and the most recent port being Shanghai, China, one of the largest seaports in Asia.

The fourth initiative was the Customs-Trade Partnership Against Terrorism, or C–TPAT, and that is our partnership with the private sector, with the major U.S. importers, with ocean-going carriers and others that own, operate, or are key participants in the supply chain from overseas to the United States. Today, C–TPAT has more than 5,000 certified C–TPAT companies who have, I submit, increased the security of the supply chain, literally from the foreign loading docks of their foreign suppliers to U.S. ports of arrival, and they have done it, in part, in exchange for benefits from Customs and Border Protection in the form of faster processing of their goods on arrival.

Let me say just right out of the box here, none of those initiatives existed on September 11. All of them have been put in place since September 11, and taken together, these initiatives are part of our layered strategy and they do provide greater protection to our country against terrorist attacks, and importantly, they provide greater protection for the primary system of international trade. These initiatives help protect the trading system itself against potential terrorist exploitation.

I might add, by the way, while I didn't list it as an initiative, of course, part of our strategy, too, has been adding significant additional detection technology at our own borders, at our own ports of entry, both seaports and land ports, to better detect against potential terrorist weapons.

But CSI and C–TPAT, they are revolutionary initiatives, but they were initiatives that, in my judgment, in our judgment, we needed to move forward with, and we needed to move forward with them quickly, indeed, as quickly as possible because for all practical purposes, there was no security of the supply chain to protect essentially the movement of goods to the United States before September 11, or very little.

But these initiatives are and they were always intended to be—let me make this point very clear—dynamic and evolving initiatives that have improved and need to continue to improve. These initiatives work in concert with each other and with the National Targeting Center and with advance information and risk management.

As a result of one of the recommendations of the GAO, we have decided to, for example, reduce the credits for being a certified

C–TPAT partner. We didn't eliminate them, but we have reduced them and we have gone to a tiered system.

Let me also say that, with respect to these initiatives, I think it is important to understand that essentially as we proposed and launched them, that many people actually said that it couldn't be done. Many people said it would take years to get them done, that there were sovereignty concerns and all of that.

And I can tell you that customs agencies in other countries around the world, they use their inspectional capabilities for inbound containers. It was a revolutionary idea to say, based upon the United States making a request that we deem this container high-risk and after analysis something that should be inspected outbound, that we want foreign countries to inspect containers going outbound rather than inbound into their respective countries.

And there may be some disagreement on the percentage here, but based upon the number of containers that we have requested be inspected by our host nation colleagues in these 36 foreign seaports, those requests have been honored about 90 percent of the time. There have been occasions where we have gotten additional information from the host nation where we could actually assess the risk as not being sufficient to require an outbound inspection, and there have been—I think the point is, you have to be there, you have to work with these countries in order to make sure that we have as many of the highest-risk containers that are searched outbound before they come to the United States.

If they are not searched there, though, this is a layered defense strategy and we have mandated that every container that we deem to be high-risk for purposes of inbound, and that is every container that scores above 190 pursuant to our Automated Targeting System, it must be inspected upon arrival into the United States if it has not been inspected in an outbound CSI port.

Mr. Chairman, I see my time is up. I just want to conclude by saying that I believe that these initiatives are working. I am convinced that America is safer today because of them. I look forward to working with this Subcommittee, with the full Committee, with the Congress, with GAO to further improve, because there are some further improvements we want to make to make these initiatives even more effective. Thank you, Mr. Chairman.

Senator COLEMAN. Thank you very much, Commissioner.

I want to first talk about C–TPAT and the concern that we have. Can we have Exhibit 4[1] displayed? Let us first talk about the process by which someone becomes a member.

The concern is if there is a recognition—can we turn that sideways? Thank you.

By virtue of membership, the benefit is a diminished likelihood of inspection. Is that the purpose?

Mr. BONNER. That is the essential bargain that incentivizes the investment by private sector companies to improve their supply chain security.

Senator COLEMAN. The concern is that to receive benefits, a company provides Customs and Border Protection with their supply chain security profile. The supply chain specialist looks at the writ-

[1] See Exhibit No. 4 which appears in the Appendix on page 111.

ten information, checks various databases, and upon successful completion of this paper review, a member receives seven times as few inspections. Is that a fair summary of the process today?

Mr. BONNER. Well, before we have modified this, and we did it recently, I thought it was about six times less likely that you would receive a security inspection if you had committed to meet the security standards and criteria of C–TPAT.

Senator COLEMAN. One can talk about the number of times, but in effect, are you virtually ensuring that shipments will not be searched?

Mr. BONNER. No, by no means. But it does recognize that if you have committed—and by the way, in many instances, we are talking about major U.S. importers that we have dealt with, that U.S. Customs has dealt with for many years who are signing on the line that they are committing to meet the security criteria of C–TPAT, and that means that they are making a commitment to use their leverage against their foreign suppliers and vendors to meet the security criteria of C–TPAT.

We are actually reaching into a part of the supply chain that is beyond the regulatory reach of the United States. I want this Subcommittee to understand that. In other words, we could not even regulate what a foreign supplier does in terms of supply chain security, but large U.S. importers which are C–TPAT members have the leverage to require those security criteria to be met under their purchase contracts and purchase orders, and that is what C–TPAT companies are doing. They have committed to do that. If they are not, by the way, they are subject potentially to criminal prosecution, penalties, and the like.

So there is some measure of assurance that they have actually done what they have said they are going to do because we have dealt with them over the years. We know that they can be trusted.

Now, we haven't ended it there, as you know, Mr. Chairman. We have said, trust but verify, and I have heard the recommendations of the GAO and I believe that we need to—and we are ramping up the verifications of C–TPAT members. Right now we have about 12 percent of the U.S. importers that are certified C–TPAT members that are validated. That is to say, we have verified that they are meeting their commitments with respect to their foreign supply chain. We have another 40 percent that are in progress.

So over half of the current C–TPAT partners, we have either validated or we are in the process of validating their supply chain, and we are hiring up and ramping up the number of supply chain security specialists at Customs and Border Protection in order to be able to do this more rapidly and to make sure that the C–TPAT members out there know that we are going to validate, and frankly, if they aren't living up to their commitments, and most of them are, virtually all of them are, but the ones that aren't are going to be suspended and decertified and thrown out of the program.

Senator COLEMAN. We have a discussion about numbers here. At least as I understand it—I think Exhibit 3[1] demonstrates—that we currently have 9,011 applicants to the program——

Mr. BONNER. That is about right.

[1] See Exhibit No. 3 which appears in the Appendix on page 110.

Senator COLEMAN. I have applicants, of which 4,857 have been certified by staff members and now receive the benefits. But in terms of validation, only 546 of those certified have had their security programs verified or validated. Is that accurate?

Mr. BONNER. I think that is about right. Ten to 12 percent have had the validations completed and there are another, roughly, of the importers, another about 40 percent or so that are in progress.

Senator COLEMAN. But all those that are certified receive the benefit of participating in the program.

Mr. BONNER. That is right. We have reduced that benefit now recently based upon some of this recommendation.

Senator COLEMAN. Now you have a tiered benefit. As a result of the investigations——

Mr. BONNER. You are absolutely right. There are benefits in terms of some degree of reduced inspections because you have committed and represented to U.S. Customs and Border Protection that you have and are meeting the minimal supply chain security criteria for your supply chain back to your foreign vendor. So that is true.

Senator COLEMAN. I believe that in the two instances that the Chairman spoke of, where Chinese nationals were smuggled into this country, involved C–TPAT members. Is that correct?

Mr. BONNER. It was a C–TPAT ocean-going carrier. The importer wasn't C–TPAT nor was—but the one link that was C–TPAT there was the ocean-going carrier, in other words, the company that was actually carrying the container from—and that was from, in both cases, from the port of Shekou, which is in Shenzhen, China, to the Port of Los Angeles-Long Beach.

Senator COLEMAN. Let me go back on the validation process. Can you briefly describe that?

Mr. BONNER. Well, yes. The validation process, we try to avoid the word "audit" because it has historic repercussions for the trade, Customs audits, and this is pre-September 11, before I became Commissioner, but it usually meant months that people would be in your company poring over all of your papers for compliance purposes.

But it is a verification. The validation is a verification that you have, in fact, implemented the commitments that you have made and that you have said you are carrying out to improve the security of your supply chain, for example, that you actually do have in your purchase order contractual requirements of your foreign suppliers that it meet the security criteria that the C–TPAT importer has told it must do in order to be a certified C–TPAT importer, and that they do periodically monitor to see that their contract, that the contractual obligation is carried out.

Now, we are verifying that—that is an essential part of the supply chain—as part of our validation process, Mr. Chairman.

Senator COLEMAN. The GAO report has raised concerns that the validation process does not have any standard operating procedure. There is not a uniform system of validation. Is that a fair criticism?

Mr. BONNER. I know that there was a criticism in the GAO report, and as a result of the criticism, we have put together a validation plan and I believe it sets forth our strategy for validations,

how we prioritize validations, what we want our validators to look for.

By the way, I will agree, at the very beginning of this process that we were—how do we know what the best practices were for the supply chain security? We went to major companies and we found out what it was. We had to develop expertise in this area. I think we have a lot now.

But I believe we have met the concern of—a number of concerns that GAO raised, one of which was that we needed to have a validation plan, how we were going to go about it, what the rules of the games are. I am not saying, by the way, there can't be improvements here. Mr. Stana may well suggest some and we are interested in continually improving how we validate, and the fact that we want to validate the C–TPAT members and we have a regime now and a staffing level that is going to help us do that far more rapidly than we were able to do when we launched this program, starting with seven private sector companies that partnered with us back in December 2001.

Senator COLEMAN. Commissioner, I will sum it up this way. I understand the vision of C–TPAT is to identify best practices and then use those. The concern, however, is that you have a substantial number of operations—and they are not all Wal-Mart and they are not all internationally known operations—that receive substantial benefits prior to certification, prior to validation, and the program is expanding.

I think that is the concern in this here report, and I appreciate the fact that you are continuing to look at this, to develop a tiered system, to improve the validation process, but I think those concerned, based on the risk if we fail, and you are in a business where failure, you can't allow it. If we fail, folks are going to come back and say, how did you let this operation get through? They simply applied. It was done on paper. You never looked at their operation, never did any physical review, never did any audit, never did any validation, and they are going to be pointing right at you and I think it is going to be tough to respond if, God forbid, the unthinkable happens.

Mr. BONNER. Well, nobody gets benefits unless they have been certified, and as you know, Mr. Chairman, of the security plans that have been put forward to us, we rejected one out of five. About 1,000, we have said, no, this doesn't cut it. This is not meeting the security criteria that is required for C–TPAT.

But I understand what you are saying and we agree, I think, that we need to—actually, as a result of things that the Subcommittee and the staff has done here, I have taken a look with my staff and we have not eliminated, we have reduced the level of benefits for just being certified and moved to a tiered system so that you do get more increased benefits after we have actually validated or verified that you have met your commitments.

Senator COLEMAN. That is appreciated, Commissioner. Senator Levin.

Senator LEVIN. If you are certified but not validated, you get less benefits?

Mr. BONNER. That is right.

Senator LEVIN. You said before the changes, there was six times less likelihood of what?

Mr. BONNER. Well, if you——

Senator LEVIN. Less likelihood of——

Mr. BONNER [continuing]. Were certified, just on average—this is just taking a statistical analysis—if you were a certified C–TPAT member, you had made the commitments, said you were doing them, and so forth, it was less likely that you would get inspected. The reason is——

Senator LEVIN. Six times——

Mr. BONNER [continuing]. You got a credit. You literally got a credit against the Risk Targeting Scoring System for being a certified C–TPAT partner——

Senator LEVIN. You were six times——

Mr. BONNER [continuing]. The effect of which——

Senator LEVIN. Got you. You were six times less likely.

Mr. BONNER. Yes.

Senator LEVIN. After the changes, where you now tier the benefit, depending on whether it has been validated, if you are not validated, what is the multiplier? Are you four times less likely?

Mr. BONNER. Let me tell you what it means in terms of the scoring credit. We reduced the scoring credit from about 125 for being certified, plus you could also get a potential of even more than that just for being certified, we have reduced that down to 75. And we have done an evaluation, Senator, we have done an evaluation at Customs and Border Protection and this is our National Targeting Center, it is our Office of Intelligence, and so forth, an evaluation of looking at the various risk factors that are in our targeting rules, and there are 300 targeting rules that can fire with respect to any particular container and there is a certain level of points, if you will, that are assigned if a container—and they go from—I don't want to go into great detail here——

Senator LEVIN. Yes, I wish you wouldn't.

Mr. BONNER [continuing]. By country of origin and so forth.

Senator LEVIN. I wish you would just try to give me the bottom line. You were six times less likely to be inspected after you are validated. Before you are validated but after you are certified, is that about three times less likely, would you say?

Mr. BONNER. I can't really give you an answer. We just implemented this in the end of April and we are going to need to see how it works out. I believe it will be that there will be some degree of increased inspections over what it had been before for just being certified, and it may well be that there is some degree of increased benefits if we have actually validated the C–TPAT member.

Senator LEVIN. In terms of the number of containers coming into the country, as I understand the figures, roughly 9 million come by sea, 8 million by truck, and 6 million by rail. Does that sound about right?

Mr. BONNER. Well, it is 11 million by truck. Seven million come across the Canadian border. It is between 9 and 10 million, last year, sea containers.

Senator LEVIN. OK.

Mr. BONNER. That has actually gone up about—almost 50 percent since 2001——

Senator LAUTENBERG. That is across the entire country?

Mr. BONNER. Across the entire country.

Senator LEVIN. So we have more coming in by truck than we do by sea?

Mr. BONNER. That is correct.

Senator LEVIN. And we have about 6 million by rail, is that about right?

Mr. BONNER. That is about right. I don't have that figure before me, but there are—we do get rail cars from both Mexico and Canada, as you know, Senator.

Senator LEVIN. The program applies to all these containers?

Mr. BONNER. The C–TPAT program, yes, it does.

Senator LEVIN. Now, in terms of the—you said you can't—you do the C–TPAT by agreement with the importers, basically, and that we are able to reach back into the supply chain in ways you could not do but for that voluntary agreement with the importers, is that basically what you said?

Mr. BONNER. In essence, that is right.

Senator LEVIN. I am not suggesting we change our approach, but isn't it true that we could simply say, unless you can certify to us that you have reached back, you cannot import? Why do you just assume that we cannot enforce our rules without an agreement on the part of importers? That is a lot better way to do it, I am not arguing with that. But I am just saying the premise that you establish here, it seems to me is one I want to challenge.

Mr. BONNER. Here is the problem. Ultimately, it is—you are building in the critical foreign security—security is actually at the foreign supplier where the container is actually being loaded or stuffed. That foreign supplier, we don't have any regulatory power over that foreign supplier.

Senator LEVIN. Correct.

Mr. BONNER. As I was discussing this, and this goes back literally to October or November 2001, what do we do under this circumstance? I mean, we are going to increase security in terms of things moving through our ports, but is there a way to extend the border out and could we do this in partnership?

I will say this. It is very difficult to think of a regulatory regime that is enforceable against the foreign supplier. So you have to literally go through the U.S. importer——

Senator LEVIN. That is not my question. My question is, you could require a certification of the importer that certain protective actions have been taken by that importer, couldn't you?

Mr. BONNER. Well, yes, you could, I think, but some importers would say—if you are trying to do this by regulation, some importers will say, well, look, we can't do that. We don't have leverage over our foreign suppliers. Our foreign supplier is a big distributor in China or Malaysia and we don't have that leverage.

Senator LEVIN. You have huge leverage over them. Unless we can certify to the U.S. Customs, we ain't buying your stuff. That is huge leverage.

I just want to challenge your statement, because it seems to me it could lead to some actions or inactions on our part which I won't accept. Now, I want to do it by partnership. I would rather do it your way. But I don't want to accept the premise that you could

not require an importer to certify that he has actually achieved that same level of protection through agreement with whoever his supplier is that you can do in a voluntary way. I will leave it at that. I just want to tell you I challenge your premise.

Mr. BONNER. If you just, though, if you think about it, if you are trying to regulate, you are telling every U.S. importer, you must do this and you must establish this level of supply chain security, and there are companies, small companies——

Senator LEVIN. No, we are not saying you must——

Mr. BONNER [continuing]. Small importers that can't do that, and, therefore, can't participate in C–TPAT, either, because they are not able to do the security of the supply chain that is necessary.

Senator LEVIN. So it is a practical way to do it. It is the better way to do it. I am just saying you are not limited to do that, and to suggest that our government is limited in that way, it seems to me, is giving away much too much. We someday may have to require certification of certain things to protect our borders which does not depend upon a voluntary agreement but says, unless you certify that, you cannot bring in materials. Let me leave it at that——

Mr. BONNER. I take your point. I still think, overall, a voluntary partnership approach made a lot of sense at the time——

Senator LEVIN. I agree with that.

Mr. BONNER [continuing]. This is November 2001. I still think it makes a lot of sense.

Senator LEVIN. I do, too. I am not challenging your effort. I think it is the right way to go.

You have indicated that all of the high-risk cargoes are inspected either overseas or here, that is mandatory, is that correct?

Mr. BONNER. Yes. I probably should define high-risk, but yes.

Senator LEVIN. Yes, but, as you define it, because there was an article in the paper that suggested that you are not quite that confident that those inspections take place at one point or another. It was a *New York Times* article, I believe, that was either today or yesterday which said that Customs officials would not provide documentation to show that all the high-risk containers not inspected in foreign ports were checked once they arrived in the United States, but they said they were reasonably confident the checks had been made. Is that a more accurate way to state it, or are you more confident than reasonably confident?

Mr. BONNER. Let me tell you my view on it, the reason I do have some confidence that the high-risk containers do get a security inspection, and that is that I am going to define high-risk container—there are different ways of defining it——

Senator LEVIN. I understand.

Mr. BONNER [continuing]. But I am just going to define it right now as this is the rough cut through our Automated Targeting System at the National Targeting Center that says this container has a threshold scoring of 190 or above.

Now, by the way, you can do further analysis as to whether that is high-risk or not, but we have essentially said and implemented, and this goes back to the summer of 2002, we basically said to our ports of arrival, and that is the Port of Newark and that is the Port

of Los Angeles, that every container that scores over 190 will be inspected at the port of arrival in the United States unless it has, in fact, had a security inspection at a CSI port overseas. In other words, we are not requiring it be done twice if, in fact, that CSI inspection has taken place.

But that is why I can say with a fair degree of confidence that every container that scores above 190 and is defined as high-risk for the terrorist threat in that way is going to be screened, if not at CSI ports, and we are still trying to push that number up, but is going to get an inspection on arrival, and that is a defense in depth. We have extended our border out and we are trying to get the extended border closer to what we do on arrival. But that is why I think I can say with some confidence that every high-risk container defined that way does get an inspection, either at CSI ports outbound or on arrival in the United States.

Senator LEVIN. That is a little more assuring than reasonably confident, as reported in yesterday's *New York Times.* That is all I am saying. I am glad to hear it. You are more confident than reasonably confident. I am glad you are. I hope you are right.

I will just wind up by saying I am out of time, so we can't get into this trash issue, but I have looked at those X-rays.

Mr. BONNER. We have talked about that before and——

Senator LEVIN. We are going to have to find a way, one way or another, because it is unacceptable to have thousands of these trucks coming in. It is all anomalous cargo. You can't see it on an X-ray. One way or another, we are going to protect—we have to find a way to protect our people.

Mr. BONNER. As you know from our conversations, I don't think we should be—we shouldn't have trash coming in from Canada into the United States, but I cannot——

Senator LEVIN. Amen.

Mr. BONNER [continuing]. I cannot prohibit it. I am going to need some statutory authority to say that is prohibited material.

Senator LEVIN. If you can't reasonably assure us the way you just did on this other cargo, if you can't reasonably assure us through an X-ray, and you sure can't because it is all anomalous, then you have to tell them, hey, after this point, no more trash.

Mr. BONNER. We are running it all through radiation detection, too, to let you know, but——

Senator LEVIN. I am not talking radiation.

Mr. BONNER. I know. We will talk about that some more.

Senator LEVIN. We need your help on that.

Senator COLEMAN. Thank you, Senator Levin. Senator Collins.

Chairman COLLINS. Thank you, Mr. Chairman.

Commissioner, I want to follow up on the issue that Senator Levin just raised about containers that appear to be high-risk and have been referred to host government officials for inspection. In its report, GAO found that since the CSI program started, 28 percent of the suspect containers referred to host government officials for inspection were not, in fact, inspected for a variety of reasons. But more recently, GAO notes that the percentage of inspections has gone up to 93 percent, so we clearly are getting more cooperation from the host governments which is very important.

One of the reasons that containers might not be inspected cited by the GAO and noted in the *New York Times* story yesterday, is they have already been loaded and are on their way to our shores. That creates the worst-case scenario. So I want to follow up on your exchange with Senator Levin.

Are you saying that when you have a high-risk container that has been targeted for inspection but was not inspected by the host government, it is now inspected upon arrival?

Mr. BONNER. Yes, I am saying that. I am making an assumption that it was targeted because it had a risk targeting score for the terrorism threat of 190 or above, and I will say in each and every case—now, I mean, I can't sit here and say that somebody didn't fail in their job in some way.

But if you looked at, for example, just taking last month, April, there were—the total number of containers that scored over 190 was about 32,000, and 99.9 percent of those containers were inspected on arrival. So I do have a pretty high degree of confidence that if has been loaded and we deemed it as a high-risk, that we would get it on arrival.

Now, we are getting better, too, with the host nation in terms of getting information quicker so that we are reducing even that small percentage, which I think was not great, but that small percentage of containers that had been loaded.

And I want to point out one other thing that is important, I think, in just thinking about this issue, and that is if we have specific intelligence about a container or there is just enough risk factors that we deem it to be totally high-risk, I have no-load authority, and we have used that sparingly, but that is the authority to tell the carrier, don't load that container or unload it at that seaport. Now, we use that very sparingly because we don't want to, frankly, sour the relationship with the host nations which are cooperating with us in the Container Security Initiative unless we really have to.

Chairman COLLINS. It does look like there has been considerable progress in that area.

Is it feasible to inspect en route, to have the Coast Guard or Customs officials go out? The reason that I ask is, obviously, having the inspection occur in the host country is the best solution. Having it occur once it gets to our shores could in some cases be too late. The whole idea is to keep the danger away from our shores. Is it feasible to do an inspection en route?

Mr. BONNER. It is difficult, but we have done it with the U.S. Coast Guard. The Coast Guard boards. It has taken Customs and Border Protection inspectors on board with it because we are concerned about a particular container before it actually is allowed to come into port. Now, again, that has been relatively rare we have done that, but we have done it when there was tactical intelligence that indicated that there might be a terrorist threat with respect to containers on board a vessel that make those—not just above 190 here, but those that we are really concerned about.

So it is possible to do it. It is difficult, though, because if you have a container ship with 3,000 containers stacked on top of each other, it is very difficult to get access, to be able to open it. We

can't run it through X-ray scanning machines and so forth. So it is difficult.

We have done it. To me, that would not be the preferred solution. You are right. It is better to identify this container and have that security inspection done before it leaves the foreign port, before it goes on board that vessel. But we can do it. We have done it on a relatively few occasions.

Chairman COLLINS. Of course, our greatest fear is that a cargo container would be used to smuggle weapons of mass destruction into the United States, and some experts have predicted an attempted terrorist nuclear strike within the next decade. That is obviously a horrible scenario, but one that we need to try to defend against.

For that reason, CBP has been deploying, I understand, radiation portal monitors at U.S. seaports. I understand, however, that these portals are deployed at the exit gates of our seaports, yet containers may sit at a port for as long as 5 to 7 days before they are screened for radiation.

We know that many of our major seaports are located in heavily populated areas—New York, Los Angeles—that clearly could be targets. I am concerned that we don't do the screening immediately upon arrival as opposed to at the exit gates. Is this an issue you have looked at?

Mr. BONNER. We have looked at it. I couldn't agree with you more. There are some difficulties in how do you do this.

First of all, the thing I would like to do, and we are joining very closely now with the Department of Energy and have over the past year or so, is to make sure that their megaports program, where they have radiation portal monitors and funding to put these in foreign seaports, is conjoined with our CSI ports. And as we expand CSI ports, we not only have the large-scale X-ray machines, which, by the way, countries that want to be in CSI, they either use their own equipment—they already had it or they have purchased it. We do not purchase it for them.

But we would like to also get the radiation portal monitors overseas, at least every container that we deem to be high-risk after analysis by our CSI team goes through not just large-scale X-ray imaging, but a radiation portal monitor. Right now, it goes through some X-ray screening, but it is not as good as a portal monitor.

Now, we have also looked at this issue of how do you do this as containers are being offloaded, and we have been looking at—unsuccessfully, I will tell you, so far—attempting to get some radiation detection on the crane, literally, the gantry that loads and unloads containers, so that as you are unloading the container, you would get a determination whether it is reading radiation. As you know, most of these radiation reads, we know from our portal monitors that we have in place, are innocuous material, but you compare it with the manifest and so on.

So far, that hasn't worked out so well, and we think that, nonetheless, we have to do the best we can here in terms of being able to screen cargo containers for radiation emissions and then resolving whether that is something of concern or, as it usually turns out to be the case, not of concern.

So far, the best positioning we have for ports of arrival is as those containers are being essentially put on board trucks and moving out of the seaport. I wish there was a better solution. We sure as heck have looked at this. And I invite anybody here who has a better answer, tell us, because we are right in the process right now of rolling out the radiation portal monitors to our seaports around the country, we have many of the major terminals of the Port of New York, which is mainly in New Jersey, as well as the Port of Oakland and several other ports. So if there is a better solution, we are looking hard at it, but that is the best one we have right now.

Chairman COLLINS. That is a challenge. I am very intrigued by the idea of having the monitor built into the crane somehow. That really sounds very interesting.

As I understand it, the Department of Energy has deployed portals in only two foreign seaports at this point, is that correct?

Mr. BONNER. That is my understanding, Port Piraeus—we have CSI in Piraeus, as well—and Port of Rotterdam. We are also on CSI there. But we are working with them so they will work with us in concert here, and they are committed to doing this at the Department of Energy so that we expand the radiation portal to the other 34 CSI ports as well as the new CSI ports that we will be expanding to.

Chairman COLLINS. Is this a matter of insufficient resources to pay for these monitors to be deployed, or is it a lack of cooperation from the host countries, or is there some other reason? Two is not very many.

Mr. BONNER. No. You are going to have to ask the people at the—this is the second line of defense—mega ports initiative at the Department of Energy. I don't feel comfortable telling you. But we have offered and they have accepted that every CSI port we go to to implement CSI, that they will essentially be joined at the hip with us moving forward now, and that is very important.

And they do have funding. Ironically, I suppose, in some ways, they have funding to put radiation portal monitors at overseas ports. We don't have that funding. We don't have enough funding to totally complete our implementation plan for radiation portal monitors at our own seaports and land border crossings and the like. But we are making good progress with the funding that we have.

Chairman COLLINS. Thank you for that information and thank you for your good work.

Mr. BONNER. Thank you.

Senator COLEMAN. Thank you, Senator Collins. Senator Lautenberg.

Senator LAUTENBERG. Thanks, Mr. Chairman.

Mr. Bonner, you agreed to the fact that there were some 9 million-plus containers that come here each year. I don't know whether you are aware of it, but the New Jersey-New York port takes almost 30 percent of those containers each year. Two-point-six million out of 9 million is almost 30 percent, right? And so it is a very high volume that reaches our shore, and it has been noted by several of the other Senators that these ports are located typically in

very highly populated, densely populated places. Am I correct with my arithmetic?

Mr. BONNER. I know that the Port of New York-New Jersey is the second largest in terms of the movement of cargo containers after the port of L.A.-Long Beach. I would say that is in the ballpark.

Senator LAUTENBERG. OK.

Mr. BONNER. It is 2 or 3 million containers a year that come into the Port of New York.

Senator LAUTENBERG. I don't want a long discussion about arithmetic. It is or it is not.

Mr. BONNER. I don't have the exact number, but that is about right.

Senator LAUTENBERG. Thank you. But the volume is what I think deserves some attention in terms of grants that are given for port security. Mr. Chairman, we have 30 percent of the containers coming into a very highly, densely populated area. It is said that the distance between Newark Liberty Airport and the Port of New York-New Jersey is the most dangerous two miles for terrorist targeting in the country and there is something there that we really have to work on.

Now, what I don't understand, could you explain just this one chart that I looked at, CSI ports, it is headed, Hong Kong, Yokohama, and Le Havre. It says, percentage of exams requested that were actually conducted——

Senator COLEMAN. I think it is Exhibit 1.[1] We have it set up, Senator Lautenberg.

Senator LAUTENBERG. Thanks. So the requests are made by us, I assume, Mr. Bonner, and it says Le Havre, and I picked on Le Havre particularly because it was a place I landed during World War II and know that it was a very active harbor. But I also know that Le Havre and France have had serious problems with immigration, both legal and illegal, from North Africa, where there are lots of people who are not so friendly to us. So is the 29.61 percent the number of times that we said, we want to inspect these cargoes, and was it denied, or that they were actually conducted from the total volume of cargo that was leaving there? Is that what that is?

Mr. BONNER. Well, it could be a number of reasons for it, but I am troubled by that, the fact that usually most of these CSI ports, our requests are honored 90 percent or more of the time, and at Le Havre, that is troubling that it is so low.

Senator LAUTENBERG. I agree.

Mr. BONNER. And it is one of the most—it does stand out. It is something, by the way, we are continuously evaluating and working with the French customs authorities, and all other CSI ports, for that matter, to increase the percentage of requests that are honored, because that is the whole point of CSI. If they are not——

Senator LAUTENBERG. And it ranks comparative to Hong Kong and Yokohama—these are both very active ports—Le Havre has substantially more cargo than Yokohama and yet the inspections

[1] See Exhibit No. 1 which appears in the Appendix on page 108.

are a very low percentage of the high-risk suspected cargo. So it is a matter of concern.

One of the things that also stands high in my mind, and that is when we look at countries like Afghanistan, Egypt, Libya, Jordan, Saudi Arabia, why aren't we focusing our efforts on cargo originating in countries that pose some real threat? And again, we would have to expand our CSI initiative.

Mr. BONNER. Maybe I could put my map board on here, but that is a good question and let me just say the reason that we put CSI—there are a number of reasons, but CSI is at ports, seaports through which most of, let us say, the cargo shipments from Port Saiid, Egypt, move through, are offloaded by feeder ships onto ports in Italy, for example, where we do have CSI. Most of the—not 100 percent, but most of the shipments, let us say, out of Pakistan move through by feeder ship to Singapore, are offloaded—or other ports in Asia—are offloaded, so we are able to inspect a lot of the cargo containers that are coming from what I would call the most high-risk areas in terms of presence of potential terrorists.

Senator LAUTENBERG. And it would be unreasonable, wouldn't it, to say that every piece of cargo that leaves there has to go through some other port. That would be an awful lot of trouble in terms of cargo delay and sending economic opportunity to other ports.

But the question was asked by Senator Collins about the inspections by Coast Guard. We have a lot of lightering of cargo in, let us say, the Port of New York-New Jersey. At that point in time, would it be possible for either Customs or Coast Guard to get to those places, especially if those ships come from some of these ports, and take a look around? There is equipment that is fairly mobile that would give you some indication of what might be a threat in one of those containers.

Mr. BONNER. We would do it, if there were specific intelligence or just the risk factors were sufficient. We would figure out a way to do it. It is hard to do even on a lighter, by the way, because you want to run it through large-scale X-ray scanning machines. You can run it through radiation detection, to some extent, not the monitors, but you can have radiation detection devices.

But if I could go back, you made an interesting point. The part of CSI, thinking about what it has done, it is not just all about how many containers get inspected. We actually have the capability right now because we have built out the Container Security Initiative that if there were time of stress where we elevated the threat level, we have the possibility right now with relatively minimal disruption to require every container coming from high-risk areas to come through, to be offloaded at a CSI port before it comes to the United States. Most of them do already, but we have that ability.

And think of CSI that way, because it is designed to be essentially the insurance policy to keep the flow of trade moving, particularly if there is a terrorist attack or we move to, based upon intelligence, to a much higher threat level than we are at today. So that is exactly it. Everything from, potentially from—and I won't name the country here, but may have to go through one of these CSI ports if it is coming to the United States.

Senator LAUTENBERG. Mr. Chairman, I think it would be of interest to get an update on this program to see whether, in fact, we

have expanded the program and to say whether you are short of personnel. Do you have enough people to do all these jobs?

Mr. BONNER. Well, I heard—I can't remember, it might have been you, Senator Lautenberg, but maybe it was Mr. Akaka, but just the cost—I know the cost seems a lot to place people overseas, and it does cost more. The rule of thumb to me was two times as much, but I will have to look at those costs.

But we only have about 200 people overseas for CSI, and those are our targeters and those are the people that are getting additional information and intelligence, in some cases, from our host nation counterparts, and those are people whose job is to also essentially jawbone our host nation to make sure that it is inspecting the containers that are high-risk unless we have been assured, based upon information that the host nation has been able to give to us.

Senator LAUTENBERG. I don't mean to cut you off, but time is running here and I don't have much left. You provoked a question in my mind when you said something about the equipment in those countries that are doing the inspections and implied that you weren't sure what kind of equipment it was. Do we have a standard that we send to these countries to say, listen, this is the least effective equipment that you can use that can get certification that we will pass?

Mr. BONNER. I have seen in many cases the X-ray imaging equipment that these countries have, and I will tell you, with one exception, and I won't name the country, but with one exception, the large-scale X-ray imaging equipment that the CSI countries are actually using for these outbound inspections equals or exceeds what we have and what we use in the United States.

So I am not against, by the way, having a standard on this. I know that is a recommendation of the GAO. But it is not just about penetrating power. It is also about the mobility of the equipment and that sort of thing. It is a combination of factors.

But I am just saying, I have looked at their machines that——

Senator LAUTENBERG. But I thought in your response to Senator Levin that there was a suggestion that we didn't know in each case what kind of equipment or whether the equipment was sufficient to give us any security.

Mr. BONNER. We know exactly what the equipment is. We have assessed——

Senator LAUTENBERG. Every country?

Mr. BONNER. But we haven't said that you have to meet these precise standards or specification. We know that in every country, it equals or exceeds what we have in terms of our own NII equipment——

Senator LAUTENBERG. So if ours is poor, theirs is poor?

Mr. BONNER. Except for one, and we are working on that country. But they are paying for the equipment. We are not buying it for them. So there is a certain amount of chutzpah to say, you have to do X, Y, and Z, particularly if the equipment—and as I say, I personally examined—not that I am the expert here, but our teams that go over for CSI examine and make an assessment——

Senator LAUTENBERG. I wouldn't think it was too nervy to say, what kind of stuff have you got?

If you would, Mr. Chairman, the country unnamed in public here, if it could be named under an executive commitment from the Chairman, I would like to know which of the countries——

Mr. BONNER. I will——

Senator COLEMAN. I share that concern and we would like to get that information, Commissioner.

Senator LAUTENBERG. Thanks very much. Thank you, Mr. Bonner.

Senator COLEMAN. Just to follow up on Senator Lautenberg's question about standardized equipment, I understand that there isn't a standard, but your testimony is that with the exception of one country, the standards equal or exceed ours.

First, my concern is that this program, CSI, is only in the end as good as its weakest link. If there is a weak link, we could pay a price for that.

As I understand from reports that I have read, the equipment that may meet or exceed ours are the gamma imagers, but in terms of radiation portal monitors, are there any standards that you are aware of?

Mr. BONNER. Well, on the radiation portal monitors, I addressed that. What we have done and what we need to do is to link the Department of Energy, their funding for radiation portal monitors overseas. This is their megaports initiative with CSI. We have met with the Department of Energy a number of times. They are committed to doing this and we are doing it. And so that would be the radiation portal monitors, then, as we join them into the array of detection technology for at CSI ports, particularly for potentially high-risk containers.

Those portal monitors are essentially the type of radiation portal monitors that we are deploying. We have deployed almost 500 of them now to our land border ports of entry and we are making great progress with our seaports. That is the best available technology there is in terms of being highly sensitive to be able to detect against even potentially nuclear devices and/or materials that could be used to make nuclear devices.

We are working, by the way, on some advanced technology which we hope to have within about a year or so. It is essentially highly sensitive radiation portal monitors that can detect even fairly low energy emissions of both gamma and neutrons.

Senator COLEMAN. I understand that there are supposed to be minimum standards—supposed to be—and I think the information we got from the agency, that a number of items a prospective CSI port must commit to, ability of their customs to inspect cargo exiting or transiting their country, access to and use of the non-intrusive inspection equipment, willingness to share trade data and intelligence.

I believe the GAO report, and I know that this Subcommittee's investigation found several countries not complying with some of these minimal standards, instances where countries were unwilling or unable to share intelligence, did not have the non-intrusive equipment or were using substandard equipment, and some lacked the authority to search U.S.-bound cargo that was transiting their ports. Would you disagree with that assessment?

Mr. BONNER. As broadly as you put it, there are issues that we are working with with various countries. Not all of them, some of them have been extremely responsive and receptive, but there are some situations where they have agreed to acquire NII equipment but they haven't—we have seen the purchase order, their government is buying it, but they don't have it there. But there is NII equipment. In some cases, we loan them NII equipment for some developing countries.

So you can't be in CSI. It is not operational unless you have the large-scale X-ray imaging equipment. So all of them have it.

Now, I mentioned the one country that we are—their equipment that they had purchased isn't where we want it to be and we are working with that country to upgrade its NII equipment.

Senator COLEMAN. CBP enters into declarations of principle with the host country? Shouldn't you incorporate minimal standards into these declaration of principles. And if they are not going to share or can't share intelligence or they don't have the equipment, simply say that they are not a CSI operation. Otherwise, how do we have any assurance that we are getting adequate inspections if you don't have these kind of uniform standards that are critical?

Mr. BONNER. We definitely need the uniform standards. I totally agree with that principle. But the way we do it, I believe, is we work with the host nation, but if we can't resolve an issue, we withdraw CSI. And CSI is very important economically to the countries that have implemented CSI because they are protecting their trade lanes, literally, between their foreign seaports, whether that is Rotterdam or Singapore, and the United States, and they understand that.

So I believe we can get—some of these CSI ports we just got online in the last 2 months, in Dubai and Shanghai. Some of them, we have had for a while. But we work very actively with the host nation, and ultimately, we may clear what it is that they need to do to be a CSI partner with us. And I believe we can get there. But again, it is a matter of dialogue. It is a matter of working with many different foreign governments and foreign customs administrations.

So I believe we are making good progress here. We do regularly evaluate where we are with respect to each one of these CSI ports through our management team here at Customs and Border Protection headquarters.

I am not disagreeing with some of the conclusions there. They are probably right. Some of them, we have been able to correct. Some of them, we are moving forward on. Some of them, as Senator Lautenberg pointed out with respect to Le Havre, even though France was the third country to sign a CSI agreement, a declaration of principles with us, some of them are not sufficiently honoring our request to inspect, do a security inspection of high-risk containers before they leave foreign seaports. We work that number up, but if it doesn't ultimately get to where it needs to be, then, of course, they are not meeting the CSI commitment and we will have no choice but to—and we are reluctant to do this, but we will essentially withdraw and we will not have that port as a CSI port unless they are meeting their commitments.

Senator COLEMAN. And you have made it clear in your testimony that there is a significant economic advantage for these countries to have a CSI port. I suggest, Commissioner, we can do better than making it clear. We can make it mandatory. We can say, this is what we are going to require, or you are not going to get the economic benefit.

Mr. BONNER. Yes. We could go back on that. We wanted the declaration of principles to be the principles of CSI and not get into all of the specific details, let us say standards and that sort of thing. There was a reason for that. There were two reasons for it. One is Circular 175 authority, and that is once you say it is a formal agreement, we have to go through the State Department.

It takes a lot longer to even get an agreement in place. Second, when you start negotiating all of the specific terms with countries—we tell them exactly what is expected, by the way. When you start negotiating it and trying to put that in a written, let us say, agreement, it takes—it would have taken a lot, lot longer. Now, it might well be that at this point, we can circle back and say we need to definitize those commitments better, whether that is through an agreement, whether that is through some side protocol for the declaration of principles. And it also has to be the same for every country that is participating in CSI.

Senator COLEMAN. And the concern is if it isn't the same, you are really getting varying degrees of reliability on these inspections.

Mr. BONNER. Well, if you don't have the right—let us say the one country which its equipment may not be all we would like it to be, if we are not satisfied with the X-ray scan or image of the container, and based upon all of our information we think it is a high-risk container, we are not able to rule it out, we will ask for physical inspection, and we do and we get physical inspections.

So there is—again, that is more time consuming, more laborious, and the host nation is doing it. But we get physical inspections when there is an anomaly or when—which is in a relatively small percentage of the containers that are run through X-rays—or if you don't have an adequate X-ray machine, then we—the recourse is to do an actual physical inspection to make sure that the container does not contain a terrorist weapon.

Senator COLEMAN. If we could get Exhibit 1,[1] the exhibit with Yokohama and Le Havre and the other ports. Just two questions regarding that.

The green, the higher risk, the number for Hong Kong being 15,000, a little over 15,000, Le Havre, 4,259. Is your testimony that those that are high-risk that every one of those 15,129 containers are checked in this country, if not inspected abroad.

Mr. BONNER. At least on arrival, if they haven't been security inspected at a CSI port. And, the high-risk, the thing about talking about CSI, we didn't start off with CSI. We actually started off with saying, let us have an automated system that uses strategic intelligence for purposes of what containers we should inspect at our ports of entry, and let us do it on a national basis and let us just say that if something scores above a certain level, that is going to give us at least a broad enough concern that we want it in-

[1] See Exhibit No. 1 which appears in the Appendix on page 108.

spected on arrival. That is what we did first. Then we expanded our border out with CSI.

But, yes, that is a very high number because Hong Kong is a port, the largest port in the world. It is responsible for shipping 10 percent of all of those 9 million containers to the United States come from or through the Port of Hong Kong. So it has a huge number of containers and it has a huge volume.

The CSI team there made 1,086 requests of Hong Kong Customs and Excise that they do a security inspection. I am not totally happy with that number, but 832 times out of roughly a thousand, they did, so 80 percent. We would like to get that higher. Our CSI management team, some of whom are behind me right now, work to push that number up so that our request, when we say we are sufficiently concerned about this container that we want it inspected, is closer to 100 percent. I mean, that is what we are looking for. There will always be some reasons why we probably won't reach 100 percent, but——

Senator COLEMAN. Let me ask another question about the high-risk containers that are supposed to be checked here. Our investigators looking into that, we were not able to either find a paper trail or anything to actually confirm that they were inspected here. And so I would ask if you would supply that to this Subcommittee. How are you sure that, in fact, those that are identified as high-risk are, in fact, inspected when they arrive here?

Mr. BONNER. Well, I am assured because—as assured as one can be, as the Commissioner, because we have mandated that at our ports of arrival, that every container that scores above 190 will be inspected, and we started that essentially in about the summer of 2002. So if we can't get it over there—and this is before we had a single CSI port. The first CSI port came online in September 2002, and that was Rotterdam.

So we started that program, and we never said with CSI, look, we are using host nations' equipment, we are using the host nations' resources, we are kibitzing whether we think that their X-ray scan shows an anomaly or not. We have never said that we are going to get total equilibrium. By the way, I would like to see that, where we are actually getting everything above 190 that would be given a security inspection overseas at a CSI port.

But what we have said is after getting the 190, we have our targeters there. We do further analysis. We do get information, by the way, in many instances. I am not saying it is perfect in every country, but we do get information that provides us additional input as to whether a container is a potential risk or it is not a potential risk. Sometimes this is just the—it is the customs authority getting on the phone and saying, well, we have a freight forwarder here. Who is the real shipper? Who is the real party and interest, that sort of thing, just getting additional information to make a more—a better assessment of what is the highest risk, basically, and then making that request to the host nation that would do it.

Now, if we need to at time of stress, this system is in place. It is not like we have to build it. We don't have to build the cockpit doors here. These are the cockpit doors for maritime security. It is

there. If we have a time of stress, we can increase the level of our request and require and demand, for the reasons you are saying.

And what is our ultimate lever here? You don't do it, the Commissioner is exercising no-load authority. It is telling the carrier they cannot put that container on board the vessel.

So we have a way of ratcheting this up, particularly at a time of stress. So view it as a security system or a piece of an overall security system——

Senator COLEMAN. And time of stress, what do you mean by time of stress?

Mr. BONNER. By time of stress, I mean there is a terrorist attack that might have been using the maritime cargo system in some way. There is significant intelligence that indicates that there is a significantly high risk of terrorist exploitation of a, let us say, the Trojan Horse, an oceangoing cargo container to carry a weapons of mass destruction. That is a time of higher stress, and we now can ratchet the system up or we can just say, you don't do it. The containers are staying at the CSI port. They are not getting loaded.

So that is what I mean. It is a system that is—it does what it does right now, and it does add security right now because it has the capability of detecting and, therefore, preventing and deterring, I believe, global terrorists, al Qaeda, from exploiting this system. It has some deterrent effect. But it is also a system that can be elevated when we need to do so.

Senator COLEMAN. I would still maintain that we have a system with some holes in it.

Mr. BONNER. I wouldn't want to—I don't rely totally on CSI. That is why we have a layered and a number of initiatives that are—that in combination give us greater assurance. But if the—nobody can say that you can develop a foolproof system, or at least a foolproof system that would not, in essence, choke off and stave off the flow of legitimate trade and do enormous harm to our economy.

So whatever system we have to put into place, there is some balancing we have to do and should do to protect, as I have said, the American livelihoods as well as American lives. You have to balance that out as you do it. But part of that is extended border strategy, and CSI and C–TPAT are very much two of our important initiatives in terms of extending our zone of security beyond our little ports of entry and our border.

Senator COLEMAN. Senator Carper.

Senator CARPER. Thank you, Mr. Chairman, and Mr. Bonner, welcome. Looking around at these empty seats, you wonder where everybody is. We all have other hearings that we are trying to get to, as well. I have two others and I apologize for not being here to hear all of your testimony.

Let me start by just asking, what are some of the possible consequences of our not doing a good enough job to reduce the security threats that our Nation faces that flow through our ports? What are the possible consequences of our not doing a good job?

Mr. BONNER. They are great. A number of people, like Steve Flynn, who is going to testify for this Subcommittee this morning, who I talked to shortly after September 11, have outlined the—if there is a terrorist incident or a terrorist attack that utilizes, let

us say, an oceangoing cargo container and we have no security system in place, the consequence was clear, and that is the whole system shuts down. It freezes, which would very likely send the U.S. economy in a tailspin and bring the rest of the world economy down with it.

So those are huge consequences, no doubt about it. The question is, how do you build, and that is the question I faced shortly—starting on the morning of September 11 and September 12, is how we would do this—how could we best do this. We are not complete yet, but how could we best do this in terms of building out a strategy that involves a number of initiatives, not just the two we are talking about today, to make it far more difficult, far less likely that this system can be exploited.

I don't think there is a perfect system that I am aware of. If somebody can devise the perfect system for providing the absolute security in terms of the movement of goods and cargo and at the same time do that without essentially choking off the flow of trade and the economic consequences of that, I am here to learn and listen, as I have been all along. But we have taken steps that are really some revolutionary initiatives.

Senator CARPER. Let me just follow things here.

Mr. BONNER. Yes.

Senator CARPER. What are some of the things that you think we are really doing well?

Mr. BONNER. Well, I think the things that we are—first of all, I would say I take it in layers. The very first thing we did was to say—and I said in talking to our people at U.S. Customs, we need to have some ability to sort out what may be a terrorist threat and what may not be a terrorist threat and we need to use advance information that we get electronically and automated targeting—we have to build our Automated Targeting Systems to do this.

We have to establish a National Targeting Center so that we can—somebody said, well, you are only inspecting 5.5 percent. The question is, we are inspecting those not on a random basis, but on a basis using strategic intelligence as to what poses a higher risk. We know that some shipments pose no risk whatsoever. So how do you do that, though? How do you make that sort?

And the very first thing we did, and I think we—by the way, it hadn't been done by any country before, but it was to build—essentially mandate that we had to get advance electronic information about every single cargo shipment to the United States. Then we had to evaluate that against our historic Customs database in terms of things that would be unusual or anomalous about shipments, build in strategic intelligence about where the threat is, what countries are more likely to be a threat than others, and risk manage the terrorism issue.

So I think that is not done, either. I mean, that is an evolving thing. We literally meet daily to assess intelligence that might and many times does change our targeting rules or tweak up our targeting rules that we use to decide which containers to inspect or not.

The next thing, though, we did was to say, look, we don't have enough people or detection technology at our ports of entry. That is why our ports of entry froze on September 12 and September 13,

because if you increase inspections and you don't have enough people to keep all lanes open 24/7, you increase inspections, you don't have any detection technology so you are able to do it faster and speedier, your border is not going to be fluid. You are going to end up damaging the economy.

And so we have added enormous detection equipment, both, by the way, large-scale X-ray imaging machines at the Northern border with Canada, at our major entry points, at our seaports, that didn't exist—weren't there before September 11. We have added radiation portal monitors. Ninety percent, right now, of the commercial trucks that come from Canada into the United States go through a highly sensitive radiation portal monitor. Eighty percent of all of the passenger vehicles, the SUVs, the cars, go through radiation portal monitors. We will have 100 percent of the Mexican border done this year with radiation portal monitors. We have about 50 percent now. We are rolling out to the seaports.

Look, I think that is an important step. It is giving us a better way to detect against potential terrorist weapons, but to do it without laborious manual inspections of everything that would shut down our ports of entry, in my judgment. Now what we are talking about at this hearing is what have we done to extend our border outward and the two very key initiatives CSI and C–TPAT, that we put into place to do that.

Senator CARPER. That may fall into my last question, and that is what are some of the quick layers we need to do better where we could be helpful?

Mr. BONNER. I think one area that we do need to be better, to do better, and we have been talking about it at this hearing, and this Subcommittee and GAO and the staff here have been helpful, but the C–TPAT program is a trust-but-verify program. We are doing better with our validations, or verifying that the supply chain security commitments have been met. But we understand and we agree that we need to do more and we need to do more more quickly, because we do give a certain level of benefit, even though we have reduced it somewhat, to companies that we think are reliable and trustworthy who are certified, that is to say, they have told us that they are doing what they say they are doing in terms of supply chain security.

But that is an area, look, it needs improvement. We do need to—and by the way, we work on this literally every day. We do need to elevate, make sure that we are getting an even higher percentage of our request at CSI ports that are honored, that is to say that the security inspection is done by the host nation. We are above 90 percent now, I believe, or an average of 90 percent—don't hold me to the exact figure. But we have steadily moved that up. There are a few ports that are laggards and we need to—we are working to get that up, and our goal is to get pretty close to 100 percent, if not 100 percent, of all the requests of outbound containers unless there is some really good reason why it can't be done.

Senator CARPER. Is there anything in particular that Senator Coleman needs to be doing to help get this job done? [Laughter.]

Mr. BONNER. Look, I think this Subcommittee and the Chairman have been very supportive, but that doesn't mean that—I do not believe in oversight. I think it is a healthy thing that questions get

asked. I want to make sure that if it is put in the right context, that people understand what we did, why we did it when we did it, and how fast we needed to do it, but on the other hand, these initiatives, I think, are good initiatives, but they can be improved. We want to work with the Subcommittee and GAO to make sure that we implement what are, I think, certainly in the main very sound recommendations that are going to help us make these programs better.

Senator CARPER. Mr. Bonner, thanks very much, and Mr. Chairman, back to you.

Senator COLEMAN. Thank, Senator Carper.

Commissioner, I want to thank you for your appearance today. I do want to add my voice, by the way, to the concerns raised by Senator Levin regarding trash coming in from Michigan and the inability to sort out what is in there, whether there are things in there that could be very dangerous for all of us. So I would seek your personal assurance that you will work with this Subcommittee, work directly also with Senator Levin to see if we—not if we can, we have to improve that situation or fix it.

Mr. BONNER. I agree. I share the concern, so I will work with you and Senator Levin on that issue.

Senator COLEMAN. Thank you very much, Commissioner.

Mr. BONNER. Thank you. Thank you, Mr. Chairman.

Senator COLEMAN. Now, I would like to welcome our final witnesses for today's hearing, Richard M. Stana, Director of Homeland Security and Justice Team at the Government Accountability Office; Retired Coast Guard Commander Stephen E. Flynn, currently a Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations in New York City; and Stewart Verdery, a principal with Mehlman Vogel Castagnetti, Incorporated, here in Washington, DC, and the former Assistant Secretary of Border and Transportation Security Policy for the Department of Homeland Security.

Gentlemen, I appreciate your attendance at today's hearing and look forward to your testimony and perspective on CBP programs discussed here today as well as your recommendations for securing maritime trade and the global supply chain.

As you are aware, pursuant to Rule 6, all witnesses who testify before this Subcommittee are required to be sworn in. I would ask you to please stand and raise your right hand.

Do you swear the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. STANA. I do.

Commander FLYNN. I do.

Mr. VERDERY. I do.

Senator COLEMAN. Please limit your opening statements to 10 minutes. Your entire statement will be entered into the record in its entirety. If you can follow the amber lights, you will know time is about up.

Mr. Stana, we will start with you. We will then go to Commander Flynn and then we will go to Mr. Verdery. Mr. Stana.

TESTIMONY OF RICHARD M. STANA,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. STANA. Thank you, Mr. Chairman. I appreciate the opportunity to appear before you today to discuss the results of our reports on the C–TPAT and CSI programs.[2] As you know, these programs are key elements of CBP's multi-layered strategy to address security concerns posed by the 9 million cargo containers that enter U.S. ports each year. Getting these programs right is important if we are to prevent terrorist weapons of mass destruction from entering the country. In my oral statement, I would like to highlight some key points we make in those reports, starting with the C–TPAT program.

C–TPAT membership is open to all components of the supply chain, including shippers and importers. In return for committing to making improvements to the security of their shipments, C–TPAT members receive a range of benefits which significantly reduce the level of scrutiny provided to their U.S.-bound shipments. These benefits can reduce or eliminate inspections at the ports and reduce wait times for members' shipments. While this arrangement seeks a reasonable balance between enforcement and trade facilitation, CBP's process for verifying the members' security arrangements has several problems that could increase security risks and throw the intended balance a bit off center.

The first problem is that CBP awards the benefits which reduce or possibly eliminate the chances of detailed inspection at the ports without verifying that members have accurately reported their security measures and that they are effective. When companies apply for the program, CBP reviews their self-reported information about their security processes and checks their compliance and violation history in various databases. If it certifies a company after this indirect review, which it has in most cases, the benefits begin in a few weeks.

Since the program's inception in 2002, CBP has directly reviewed and validated members' security procedures for only about 11 percent of the companies it has verified. More importantly, this figure goes down to 7 percent of the certified importers, and this group of members receives the greatest number of benefits. Moreover, it is unclear whether the other 89 percent could have serious vulnerabilities in their supply chain security and still be awarded program benefits.

The second problem is that the validation process itself is flawed. For the 11 percent of companies that have been validated, CBP did not take a uniformly rigorous approach to reviewing the security procedures. Validations are supposed to verify that security measures are in place and are effective. However, CBP typically examines only a few facets of member security profiles and CBP and the company jointly agree on which security elements are reviewed and which locations are visited. In some cases, the majority of a company's overseas supply chain was not examined.

---

[1] The prepared statement of Mr. Stana appears in the Appendix on page 66.
[2] See Exhibits No. 8 and 9, which appear in the Appendix on pages 115 and 154 respectively.

Further, CBP had no written guidelines to indicate what scope of validation is adequate nor a baseline standard for what minimally constitutes a validation. C–TPAT program officials say that validation is not intended to be an audit of voluntary members, but the review that is done does not always add up to a reliable assessment of supply chain security.

A third problem is that CBP has not determined which and how many members need to be validated and how many staff it needs to devote to this important activity to mitigate security risks. Although it initially intended to validate every C–TPAT member, CBP devoted an inadequate number of staff to do that. In August 2004, it began using what it calls a risk management approach to prioritizing which members should be validated first, as resources allow. CBP has established some selection criteria, such as import volume, value of imports, and method of transportation. While this is a step in the right direction, CBP still needs to determine the validations that are needed to help assure that members deserve the benefits that they are awarded.

CBP is addressing the management weaknesses we noted in our July 2003 report, but it still has a ways to go in some areas. It hasn't yet completed a human capital plan and it hasn't developed its performance measures fully and importantly. Our review disclosed that its basic records management system was in such poor shape that we could not rely on it to gauge program operations or reconstruct management decisionmaking.

Turning now to the CSI program, we found some positive factors that have affected CBP's ability to target and inspect high-risk cargo shipments at foreign ports before they leave for the United States. Among these are improved information sharing between CBP and foreign customs staffs and a heightened level of bilateral cooperation and international awareness of the need to secure the whole global shipping system.

However, our work also disclosed several significant problems in the CSI program. One problem is that about a third of the cargo containers leaving CSI ports are not fully screened before they depart. This is because diplomatic and practical considerations made it very difficult to fully staff certain ports to the level prescribed in its staffing model. This has limited CBP's ability to screen all shipments leaving some CSI ports.

Also, CSI hadn't yet determined which duties require an overseas presence, like coordinating with host government officials, and which duties could be performed in the United States, like reviewing manifests and databases. Given the diplomatic and logistical consideration and the high cost of stationing staff overseas, CBP needs to consider shifting work to domestic locations where feasible.

Another problem is that not all cargo containers that are screened and referred to host nation customs officials for inspection are actually inspected before they leave the ports. Reasons for not inspecting these containers include the availability of host nation information that suggests that a container might not pose a security risk, the host nation's customs officials could not get to the container before it left the port, and in 1 percent of the cases, a

host nation inspection denial, most often because the risk identified relates to a customs violation rather than a security concern.

Our audit check of a 3-month period found that CBP can and does inspect most of these potentially risky containers when they arrive at U.S. ports. However, we were unable to verify that 7 percent of these containers that were referred for state-side inspection were actually inspected upon arrival. I think this might have been a point of confusion in Chairman Collins's note that 93 percent were inspected. That number was not the percentage inspected at CSI ports. That was the ones that were not inspected at CSI ports and referred to U.S. ports for inspection and documents show an inspection was done. As the Commissioner mentioned, CBP also has issued "do not load" orders in a few cases where it felt strongly about the need to inspect a container before it arrives at a U.S. port.

A third problem involves the lack of minimum technical requirements for inspection equipment. Both CSI ports and U.S. ports rely heavily on non-intrusive inspection equipment, such as various types of X-ray and gamma ray imaging machines, to conduct inspections of cargo containers. Equipment used at various CSI ports can differ in their penetration capabilities, scan speed, and several other factors. Without minimum technical requirements, CBP has limited assurance that the equipment in use can successfully detect all weapons of mass destruction. It is important that CBP establish such requirements because non-intrusive inspections at a CSI port may be the only inspection some containers receive before they enter the interior of the country.

Finally, CBP has made several improvements to the management of the program, but some problems still exist. To its credit, it has made some progress developing a strategic plan and performance measures, but further refinements are needed, particularly with developing meaningful measures of bilateral progress, terrorism deterrence, facilitating economic growth, and not disrupting the flow of trade.

In closing, we made a number of recommendations aimed at addressing procedural, staffing, technical, and management problems we identified in the C–TPAT and CSI programs and we are encouraged by the constructive tone of CBP's response. It is very important to resolve these problems as soon as possible, because in CBP's multi-layered strategy for mitigating the risk of a weapons of mass destruction being transported in cargo containers, any weakness in one program or layer could affect the other layers.

Mr. Chairman, this concludes my oral statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

Senator COLEMAN. Thank you very much, Mr. Stana, and thank you for the good work being done by the staff and the folks at GAO on these reports. It has been very helpful and really outstanding, so I just want to say thanks.

Commander Flynn.

TESTIMONY OF STEPHEN E. FLYNN,[1] COMMANDER, U.S. COAST GUARD (RET.), JEANE J. KIRKPATRICK SENIOR FELLOW IN NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS, NEW YORK, NEW YORK

Commander FLYNN. Good morning, Mr. Chairman. It is an honor to be here this morning to talk about this absolutely vital issue. I really want to commend you and the Subcommittee and the Committee for taking the container security issue on.

I have been somebody who has been working the container security issue for well over a decade. I want to start by saying this has been a longstanding vulnerability which went largely unrecognized prior to September 11. Even in the immediate aftermath of September 11, there was not a whole lot of activity happening across the U.S. Government, and I commend Commissioner Bonner for grabbing this issue when the Department of Transportation was otherwise focused on aviation and when the Coast Guard focused on ships and terminals but wouldn't go after the cargo issue. That leadership should be applauded.

But, of course, where we are at right now is how to deal with an issue of enormous stakes, as we have been talking about, and how we can move this thing forward. What I would like to do in the few minutes I have here to provide oral testimony, is talk about the stakes, my view of the threat, and how I believe that C–TPAT is missing that threat in how it is currently operating and some suggestions, recommendations on how we could move forward.

I think the best way to illustrate the stakes is to bifurcate them in two parts. One is that the container system, the intermodal transportation system, could be a conduit for a weapons of mass destruction. That is the one that consumes the bulk of our attention. The second issue is that the system itself is targeted, our trust in it erodes, and we stop using it for a while, and that could potentially lead to a global recession.

Now, those stakes are, I would argue, national security imperatives of the first order. We have to deal with those two problem sets. But the best way to illustrate the second one is to visit a place like Hong Kong, the world's busiest container port in the world and the busiest terminal there is one called HIT Terminal. I was there a little over a year ago with the brilliant Malaysian who designed the operation of that terminal in 1992 to handle 3.1 million containers per year.

Today, HIT Terminal is moving 5.5 million on the same footprint, on the same square acreage. That entails 10 Panamax or post-Panamax container ships being loaded simultaneously with 3 to 4 gantry cranes per ship, 35 moves per crane per hour, 24 hours a day, 7 days a week, 365 days a year. He quipped that "we no longer take off Chinese New Year." There is a 1-hour slippage time between ships.

Now, when something goes wrong, such as the computers go down for 30 minutes, they will snarl truck traffic throughout the Port of Hong Kong. If it goes down for 2 hours, the trucks back up to the Chinese border. A little over a year and a half ago, they told me they had a typhoon come through where they had to shut the

[1] The prepared statement of Commander Flynn appears in the Appendix on page 94.

port down for 96 hours and they had a 140-mile backup of trucks. Between 16,000 and 18,000 trucks were queued up into the Chinese mainland.

This is a system of incredible fragility, that if we have a disruptive event, the cascading effects are immediate and have significant economic repercussions.

Now, it is also, therefore, a system that is very difficult to police. C–TPAT and CSI, of course, are designed to help advance that. The concepts of obviously targeting before it is loaded and getting the private sector to be a partner in this process makes sense. The critical issue that I have separated myself from where CBP is going with this is the notion that CBP can identify the right 5 percent and put this through the scrutiny of, to put it in the words of Commissioner Bonner, the 100 percent of the right 5 percent and presume the other 95 percent is low-risk and does not require inspection, whether overseas or even here at home.

The central problem with this premise is that its view is that CBP has the ability to identify this high-risk universe, which would clearly require that CBP has a level of intelligence CBP does not have for this adversary.

But second, it is that Customs believes that that universe where the terrorists are most likely to exploit would be the places that make up the shadow world CBP has learned about by failure for customs compliance in the past with trade laws and so forth, new players we don't know much about, so they have no track record, or they have had a history of smuggling before. The assumption is that a terrorist intending to bring in a weapon of mass destruction into the United States would gravitate towards the place where CBP already sees aberrant activity. That is what CBP targets. CBP inspects that, but assumes that terrorists wouldn't gravitate to legitimate companies.

Where I would argue that this is wrong-minded is that in the case of a smuggler, it is an ongoing conspiracy. He has to be in the shadow world. He does not smuggle drugs in once, or he does not violate a revenue law once. He does it as an ongoing conspiracy. And if he goes to a legitimate company, they have controls and over time, and he is going to get caught. So that doesn't make any sense.

That is a different problem from the lower-probability, high-consequence risk of a weapon of mass destruction being put in the United States with the goal of setting it off. In that situation, he is happy to succeed once, and it may have taken him 2 or 3 years to acquire the weapons. And so if he is somebody who is interested in carrying out the strike and CBP has already advertised up front that this legitimate company's 95 percent universe is viewed as low-risk and not subject to even the most cursory inspections, that is where he will focus his attention and he is going to take the time to do it.

It turns out we are expecting too much from private sector companies to secure themselves with a fail-safe approach. Security in any private sector, if you talk to any chief security officers as I do, is much like other audit systems. You look for behavior over time. A good security system is one that has trip wires in the company to see whether or not the rules are being violated, has an investiga-

tory arm to go out and check on the behavior, has a sanctions system for people caught violating the behavior that sets a deterrent across the company that employees should play by rules or you are going to have a consequence. You are going to go to jail or you are going to lose your job. It is a reactive system, in other words. No system is designed to protect the system for the first offense.

Basically, bringing a weapon of mass destruction into the United States in the 95 percent universe CBP is defining as low-risk is as simple as a large payment to a truck driver to take an extra-long lunch break so as to gain access to that load, and you are on your way.

So my concern is, not that we are getting companies to be a partner in this process, but that automatically creates this 95 percent low universe that doesn't warrant CBP checking. Even today, CBP focuses their attention on the high-risk universe of what CBP has found these problems. But I am very concerned about this 95 percent low-risk, and let me push it a step further.

It is not only that I believe that it is the richest opportunity for somebody to get in once, into the United States to cause this event. I also believe that—and this takes a little more sophistication on their part—if the goal is mass economic disruption, the kinds of things Osama bin Laden has been talking about, they will want to strike that low-risk universe because it will then invalidate the regime, the entire—all containers will look at high-risk.

So this leads us to rethink how we do inspections. Building on C–TPAT, building on CSI, which are minimal approaches, one is we have a greater assurance that companies are living up to the security obligations. We talked about the issue of jurisdiction today being a problem, it is clearly an issue. The lack of capacity and resources is an issue. We have ways to solve this. It is called third-party independent auditors, folks who are bonded to do this job, and you audit the auditors. It is the kind of format the Coast Guard uses routinely through outfits called the Professional Classification Society like the Bureau of Shipping. Resident technical experts go out and check, and the Coast Guard check, the checkers.

Customs has been reluctant to go to this approach, and frankly, I don't understand why. It is a way you can get in overseas jurisdictions and you can have a validation process relatively quickly deployed.

The second piece, though, is that we have to move to a system where we validate low-risk as low-risk. This is not a physical inspection of everything moving through. And I want to highlight specifically an initiative that I have been involved with in the Port of Hong Kong. The Port of Hong Kong today has an initiative where every truck coming into that busy terminal, I just described, is going through a radiation portal, a gamma imaging, an optical character recognition capturing the container number and putting it into a database. Right now, there are about 180,000 images sitting in this database since January 1. Nobody in the U.S. Government has asked them to do this. It is being funded by the Container Terminal Operators Association, and a U.S. company has been involved with it, SAIC, has put the equipment together. But nobody in the U.S. Government has told them that this is desirable behavior.

Now, their interest in capturing this data up front is really threefold. One is the ability to deter for every box, that low-risk universe as well as what we would target as a high-risk universe, that it is going to get scanned and we are going to raise the risk of detection. If you spent 3 years getting a weapon of mass destruction, do you want to put it into a system where everything is getting scanned and hope it is not detected?

The second piece that makes this an attractive approach is if, God forbid, something happens, they have the black box. They have the forensic tool that you can go back and say, it came from the Port of Hong Kong but it was specifically this supply chain. We may have missed it, but here is the tape. So we indemnify the port and we isolate the problem to a supply chain. That keeps the whole megaport from coming down. The kind of dump the concourse problem we see in airports. They can avoid that.

And the last piece that has value for them is the current process of targeting, this typically requires a pulling of the box from the stack, dragging it over to the one inspection facility, putting it through the same screen that can be done up front, costing the importer the money to do it there, disrupting the terminal operation, and likely missing the voyage. And what they see as attractive about this is you can do that virtually and 99 percent of the time resolve the kind of questions that a CSI targeter would have by just looking at the image in real time, and you can look at them here in Virginia or you can look at them in Hong Kong or wherever you want to go.

That system, we could migrate globally quickly, and it is not the end of all ends, but it is a layered approach in which we move away from saying there is a very finite universe of high-risk things and instead which we apply more broadly across.

And so I would in conclusion here make the recommendation we need to be thinking about a validation process that low-risk players are low-risk. A birth certificate, the starting process, third-party independent players, a tracking as it moves through, a vetting at loading port. This is in the realm of technically possible, commercially possible. We just need to move forward aggressively.

Thank you very much, Mr. Chairman.

Senator COLEMAN. Thank you. Mr. Verdery.

TESTIMONY OF C. STEWART VERDERY, JR.,[1] PRINCIPAL, MEHLMAN VOGEL CASTAGNETTI, INC., ADJUNCT FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, AND FORMER ASSISTANT SECRETARY OF BORDER AND TRANSPORTATION SECURITY POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. VERDERY. Thank you, Senator Coleman, for the chance to be here today. As was mentioned, I am a principal at the consulting firm of Mehlman Vogel Castagnetti. I am also an Adjunct Fellow with the Center for Strategic and International Studies, but the views are my own that I will explain today, and I would just go over a couple of the key points because I know we have been here for a while.

[1] The prepared statement of Mr. Verdery appears in the Appendix on page 102.

As you know, I was Assistant Secretary for Border and Transportation Security Policy and Planning for the last 2 years, until my resignation earlier this spring. I was responsible for immigration and visa policy, transportation security, as well as cargo security, largely carried out in the field by CBP, ICE, and TSA. I would be remiss if I didn't thank the Committee for your outstanding efforts to support DHS during my tenure—the intelligence bill probably the most famous—but also your oversight responsibilities were very helpful in focusing our energies and making us do a better job.

The point of today's hearing, I think, is to understand that this is a layering of programs, and while we are focusing on two very specific and important programs, CSI and C–TPAT, they are not the only programs that are relevant and they shouldn't be looked at in a vacuum. I think Commissioner Bonner talked eloquently about the layering that CBP is responsible for, but it is really beyond CBP, and I will talk about that in a second.

I strongly disagree with any analysis, such as the press accounts we have seen the last couple days, that somehow suggests we are worse off with CSI and C–TPAT and the related programs that they undergird than we would be without them. There are minor flaws that need to be fixed—some of which already have been—due to budget or operational concerns or technology limitations or international agreements, and they have to be worked on, but that should not lead one to the conclusion that we are better off without them. It is not an either/or proposition, as the title of the hearing might suggest, and I know people make hearing titles to be catchy, but it is incremental progress that should be considered that the Department and the Congress supported their programs and we need to think of it in that light.

Now, I will say, having looked at some of the major other issues that we face in Homeland Security, we have done more in other areas to come up with an overall strategic plan. You think of visa policy, you think of entry/exit, you think of aviation security, intelligence gathering. With cargo and supply chain security, we have not really done that.

The programs we talked about are part of that, but they are not a plan in and of themselves, the programs that CBP and the Coast Guard and other parts of our government implement, and that is why, at the direction of Secretary Ridge and especially Deputy Secretary Loy last year, we were instructed in my office to build a National Strategic Plan for Cargo Security. For any of you who were at the cargo summit that DHS put on in December, you saw the first draft of that. It is a public document. That is now being reviewed within the Department as part of Secretary Chertoff's second-stage review, and my understanding is that will be something that he is focusing on moving forward throughout this summer. He is coming up with a rubric under which all programs can be handled.

Let me talk about a couple of things that are beyond CSI and C–TPAT just for a second before returning to this.

I do agree with the witnesses today. We do need a zero tolerance for weapons of mass destruction and to devote whatever energies it takes to build that into our system. It is a layered approach, but we have to have that as a 100 percent layer along the way at some

point, preferably overseas, if not overseas then domestically. And so we are moving in that direction with the procurements and the deployments we have talked about. I think it is absolutely critical that we rely on our Science and Technology Directorate who has come up with a procurement announcement earlier this year to get the best equipment out there and to have standards.

I also would encourage the Congress to support the proposed Domestic Nuclear Detection Office, the DNDO, as a great opportunity to coordinate efforts that do cross agencies within DHS and even beyond DHS in this absolutely critical area.

The second phase that is beyond these programs is the Maritime Domain Awareness Effort led by the Coast Guard and the Navy under Homeland Security Presidential Directive 13, signed last winter. This will bring visibility into shipments between when they leave a foreign port and when they arrive domestically. Couple that with the improvements in in-transit protection that we need, first, a regulation that is in the works on mechanical seals, subsequently with high-tech seals or so-called "smart boxes" to provide detection notification. Those are things that will bring a measure of accountability between departure and arrival that we absolutely need.

Turning briefly to CSI and C–TPAT, I completely agree with the GAO's suggestions in many respects, and I found their work to be very helpful in my responsibilities and think they do a great job.

In terms of CSI, I think that CBP does need to redouble efforts to get people overseas to support these efforts. Deploying people is not an easy thing. We worked on it in many other programs besides CSI, and finding the space to get these people overseas, getting the agreements in place with the State Department is not simple. So it does take time and people have to be somewhat patient.

I am not sure I agree with the suggestion that we should be returning those people back to the United States to do work here. Once we get people overseas and have gone to that trouble, we ought to be having them work more with host governments to develop leads, to work with local law enforcement and customs officials to figure out the best ways to make that targeting the most effective we can. That can only be done overseas, working with people on the ground.

I also would recommend that people try to make these deployments for as long a term as possible to develop those long-term relationships and not have people deployed on TDY basis.

In terms of C–TPAT, I am heartened that CBP, working with myself and Under Secretary Hutchinson, have increased the number of validators that are coming online to make the system more whole. I do agree that—and I take some blame here in not coming up with this idea myself—there should be a tiering among the companies that have been accepted or certified but not validated, and I think it is an entirely appropriate measure of risk management to have a tiering for companies that have essentially made promises that have not been confirmed.

It does strike me that these companies have track records in dealing with the government that ought to be considered and that they should be given some measure of benefit, but not the full benefits that are given to fully certified C–TPAT members.

The last thing I want to mention in my oral remarks is the need for a more broad, more expansive policy office within the Department. I noted with some irony that neither of the GAO reports even mentioned the fact that there is any type of policy oversight within the Department for CBP or any of the other agencies at the bureau level. We see that this issue really does cover issues beyond CBP's responsibilities, especially on the international front, and the reports don't even mention a DHS policy coordination effort or a BTS policy coordination effort and I think that speaks volumes of the dilemma that we have.

The work has to be coordinated between Coast Guard, between TSA, between the Science and Technology Directorate, and especially overseas, where we need to bring the full weight of the DHS relationship to bear on each of the programs. We should not be having Customs overseas negotiating separate agreements, and the Coast Guard overseas, ICE, and TSA, they need to be worked together. And so my hope and my expectation is that the Department will come up with a robust policy office providing guidance to all the operational bureaus as well as managing international affairs as part of the Secretary's second-stage review that is ongoing.

I thank you for the chance to be here today. I look forward to your questions.

Senator COLEMAN. Thank you very much for your testimony.

I want to go over a couple of things that Commissioner Bonner stated. He indicated very clearly that all high-risk containers overseas, if they are not inspected overseas, are inspected when they get here. Was GAO able to verify that?

Mr. STANA. No. In fact, of the 65 percent of the containers that were classified as high-risk and were reviewed by the staff overseas, our detailed work at the ports suggested even within that 65 percent, there is no guarantee that all those were high-risk or not high-risk. That is the first point.

The second point is when the CSI port people call the U.S. port people and notify them that they couldn't get it inspected for whatever reason, we found no records that could assure us that in all cases the inspection was done stateside. So we don't have the high level of assurance that Commissioner Bonner has.

I might add also, if you recall, about a year ago, we did some work on the ATS system and there were some problems there identifying cargo risks and making appropriate designations. This whole CSI system is predicated on ATS.

Senator COLEMAN. Explain ATS.

Mr. STANA. ATS is the Automated Targeting System, the system of rules that Commissioner Bonner was describing. There are many of them, hundreds of rules that, based mainly on manifest data, create a point score and risk designation.

We found problems with the ATS system that suggests that it also is not absolutely reliable in identifying high-risk cargo.

So you put those three together and it suggests problems. I understand where he is coming from, but I wouldn't speak with the same level of assurance.

Senator COLEMAN. Mr. Verdery says we are not worse off, but I think one of the problems here is that we have a system based on

an ATS system of which there are concerns about it, the system does a good enough job identifying the risk.

Commander FLYNN. Well, it is true that we are probably not worse off because we have these systems in place. In fact, they are good faith efforts, as you pointed out.

The problem is, is that when you rely on these systems to do the things that they are designed to do and they don't, it creates other vulnerabilities. For example, in some ports, if a container came from a CSI port, they may reduce level of inspection or eliminate it, not necessarily on a point score but because it came from a CSI port.

Senator COLEMAN. I am not arguing with you, Mr. Verdery, in terms of worse off, but I worry about a false sense of security. I worry about increased vulnerability because of reliance upon a system that, at its core, has a few challenges.

Commander FLYNN. I might just highlight, and this speaks to the need for the coordination, but the National Targeting Center, for instance, isn't hooked up to the Office of Naval Intelligence or Coast Guard's efforts to target based on maritime data.

But that targeting effort is based on prior history. CBP is really operating in terms that past performance equals future results. If you have been shipping terrorist-free for 2 years and you have been complying with Customs rules, you are viewed as no risk of terror having compromised a global supply chain. Now, that is just something that no company can achieve and one that we can't have automatic confidence in. It is not that we can't find scary places, but the underlying intelligence that goes into the ATS system is very weak, as we know from just the intelligence that we have about this adversary overall.

So it is all built on that edifice of Automatic Targeting System primarily with just applying it overseas. CBP is getting it early enough that CBP can do some analysis and ask a few more questions. But the rest of that universe is viewed as something CBP does not need to look at, and I think that is problematic.

Senator COLEMAN. I am going to come back to the issue of auditing and what that means, but I just want to follow up on another thing the Commissioner said. He was pretty confident that, with one exception, the non-intrusive equipment that is being used at the CSI ports meets or exceeds what we have here. Would you concur with that?

Mr. STANA. We are doing some work on that issue right now. We are doing a technology assessment of the different non-intrusive inspection equipment being used. But I will say this. In our classified report, you may recall a chart that we had of three different types of equipment. They had different scan speeds, they had different penetration abilities, and so on. They are not all the same. Some may be better off in some areas, some may be better off in others.

But what we are suggesting isn't so much to set a standard so that one port improves or that one country improves. What we are suggesting is, is you may want to set a standard so that you have scan speed and penetration ability that is consistent so that when you get an inspection done, it is a consistent inspection and you can have confidence in it and you don't need to reinspect the cargo container.

Commander FLYNN. Mr. Chairman, if I can on that issue, one of the biggest problems is the disconnect, between radiation portal monitors and gamma scanning and whether or not detection can happen. CBP may have good equipment, but when they are not used together, the central problem is this.

Radiation portals won't help you with shielded weapon, which would be a loose nuke. It won't help you with a shielded RDD, a dirty bomb. And it won't help you with highly-enriched uranium because it doesn't give off enough of a signature vis-a-vis the background. So to rely primarily on a radiation portal technology, it is not helping us with the scariest problem set.

But when you have a radiation portal, it forces the shielding because they know you could detect it for the dirty bomb problem, particularly. Then your imaging would say there is a big cylinder object or whatever here in the middle of a shipment of sneakers. That is a problem.

So part of the issue is DOE has been marching off deploying radiation portals entirely isolated from DHS's effort. DHS only uses the gamma for a very small population, because that is all they have the resources to do. They ask other countries to apply it in the same way. And these two worlds haven't come together.

So it is not the technology itself is a problem, it is how we integrate the technology, how we integrate it with data.

And I will just highlight another issue, keeping the information. We are not storing the information after we get these images. Storage is cheap, but CBP is tossing it away. CBP is basically throwing away a forensic tool if something went wrong, or even a tool that CBP can learn from over time. I don't understand why that is happening, but for stuff coming across the Canadian border, as soon as the image is taken, within a day or so, the image is gone. CBP dumps it. It makes no sense that CBP is not storing this and trying to learn from it, as well.

So it is the technology has limits, but it is more about how we integrate it, how we interface with software, how we use human judgment as a part of the process.

Mr. STANA. And if I could just add one more thing, most of the detection equipment we are speaking of is aimed at nuclear or radiological threats. There are other types of weapons of mass destruction that we do need to focus on and to build some standards around.

Senator COLEMAN. Let me talk a little bit about the audits. As I was listening, Commander Flynn, to your testimony, I was wondering, where are you going with it? In other words, what are you proposing? What is the solution?

Commander FLYNN. We have a system now that if you talk about the system of terrorism it is not going to be a pattern, all you have to do is one shot, you have to get it through, so the thing that we are looking at now of narcotics and other things are based on, as you said, somebody continuing to use a system and figuring out a way to avoid it. So the best targets, I think the soft targets are those operations that have been "validated," that, in effect, really almost guarantee not being checked further.

If there was one concern I had with the Commissioner—one other concern I had with the Commissioner's testimony was even

though there is a tiered system right now, the fact is that you are giving, in effect, carte blanche to companies that have not been audited, clearly not been audited.

Mr. STANA. Yes. I think that is a cause for concern. I heard the tier approach. I think it is a step in the right direction, but the fact of the matter is, with the vetting process, you are assuming that the kinds of vulnerabilities that you addressed in the past are indicative of the security chain vulnerabilities of the future, and this assumption is made without a validation. What they are doing is giving a number of benefit points to a vetted company without validation, and the number of points is sufficient to move them from a high-risk category to a low-risk category.

Senator COLEMAN. In part, is the problem of validation perhaps almost—perhaps a difference in philosophy? Customs and Border Protection isn't really talking about auditing. Even their validation is not an audit. Commander Flynn, you ultimately said that you have to audit the auditors. That is an audit.

Commander FLYNN. Right.

Senator COLEMAN. And what I am not hearing in place today is a system in which GAO actually would consider an audit.

Mr. STANA. Or at least a reasonable examination of the supply chain security. What is happening is you have the CBP and the company agree to what CBP will look at, and oftentimes, it is not the crux or even the majority of the operation, and that is troublesome.

Mr. VERDERY. If I could just suggest, I think that in my prepared remarks, I talked about the consideration of turning parts of C–TPAT into a baseline regulatory regime. Not all of it is probably suitable to go into your typical statutes and regulations, but as we load up more and more bells and whistles onto essentially a voluntary deal, I think the time has come to consider whether or not this should apply to all players, all importers and other folks in the supply chain, and also, I think, provide a degree of transparency into how these processes are done.

As I understand it, the recent changes on the tiering were announced by E-mail. I am not sure this is the way government business ought to be handled. And I do think that a regulatory baseline in some respects of C–TPAT would provide that kind of—it is not going to be an audit, but it would provide that kind of level of assurance that you might give the public more confidence.

Now, I don't think people should take too much the fact that something is validated: That is a snapshot in time. That is no guarantee that a week later, things haven't changed. So I don't think you can divide the world into black and white. These are companies we have to have ongoing relationships with and a regulatory regime might be a way to make that more productive.

Commander FLYNN. If I can, Mr. Chairman, where I am going with this is this validation is the entry-level argument, so it is the birth certificate process. Agreed-upon protocols, somebody goes out and checks that the company is actually living up to them. Sarbanes-Oxley style, basically. Are you living up to the controls? It is not done by the U.S. Government, it is done by folks who are skilled at auditing. And then DMS checks the checking process. So that is the kind of mechanism there.

But then to assure that, in fact, this is happening, that the low-risk is staying low-risk, you have confidence it was stopped, you are tracking it through and you are spot-checking along the way. It doesn't have to be 100 percent because terrorists don't have unlimited resources or unlimited weapons of mass destruction. If, in fact, it looks like the deterrent—the probability of success in the system looks not so good, even 50/50, they are going to go another route.

So by building this robustness to it—but my nightmare scenario now is the weapon of mass destruction will go off in Minneapolis and it will come via a C–TPAT company on a C–TPAT-compliant carrier through an ISPS-compliant port, an ISPS-compliant ship, and the entire regime will fall apart because we didn't build the controls in up front to give us confidence in it.

Senator COLEMAN. It is pretty sobering. I sense in your testimony about keeping data, in part what you are saying is if something does happen, you can at least identify this is the problem so that the entire system is not cast aside?

Commander FLYNN. To deal with the incident, the analogy I would use, Mr. Chairman, is the black box in an airplane. We don't put them in there because they are free and because they make the planes fly better. But every time—the rare times that jet airliners fall out of the sky, if the only thing that the aviation industry and the government did was shrug and say, it doesn't happen very often, it is one in a million times, people wouldn't get back on planes.

Having the tools and the system to verify even after, to support the investigation, so as to find an isolated supply chain that was a problem. CBP can focus on it. It means you don't have to close the border with Canada. You don't have to close the seaports around the country. But if you can't do that, you have to assume everything is at risk, and that becomes a real problem for us.

Senator COLEMAN. My problem may be definition of terms. We talk about things being certified. In the public's mind, I think they think certification has some really strong value. This is USDA-certified Grade A meat or whatever. Somebody has looked at it. Somebody has inspected it. Somebody then checked it out and they have made a judgment.

And what we are having here is we have application, certification really being looking at paperwork, just looking at paperwork and trusting—this is trust but not verify—that you got what you got. That is a far cry from certification.

And then in terms of validation, you can have validation which is not validating this is the way the system works. What you are looking at, it is the blind man and the elephant. You are literally looking at one little piece of it that may or may not be representative of the rest of the system, and you are looking at a piece, by the way, that you have agreed up front to look at.

So it is a kind of thing that FDA wouldn't do. So that is my concern, that we have phrases here—certification, validation—that I don't think meet the standard definition that most folks would think about. And again, when we go back to the risks here, they are pretty significant.

Let me ask a question, though, about validation, even the system that we have. It seems to me the program is growing very rapidly, but we are only validating a small percentage. Is that problematic?

Mr. VERDERY. They have to catch up, and I think they are catching up. Bringing on these validators, you have to get them hired and trained and the like and they are catching up. I think you heard the Commissioner say 11 percent are validated now and they have 40 percent in the works. I do think that the recruitment efforts, perhaps, ought to take a back seat for a while to the validation efforts.

Sir, if I could just—I think, essentially, you have a situation where you have an interim security clearance. We allow those in other types of situations. And the question is, do you provide any kind of benefit for somebody at that level? I think it is a reasonable risk management tool to give some benefit, even if you are not going to give a full panoply of benefits.

And again, I think people would be a lot more comfortable with this whole rubric or regime if at one point along the way there was a 100 percent check for WMD, and that, I think, has got to be a priority, to get those machines out, preferably overseas. Where we can't get them overseas, have them domestically. I think that would provide a kind of a backbone to make this thing make more sense from a logical basis.

Senator COLEMAN. Let me have Mr. Stana first, and then I want to follow up on this point.

One, this question of catching up, what is your best estimate of our capability to catch up?

Mr. STANA. It is going to take years at this rate. I mean, we are not much further along now in hiring new people than we were months ago. For that reason, a couple things have to happen. They are going to have to prioritize which ones to validate first, and I would start with the importers who are receiving the greatest benefits. And yet only 7 percent of them have been validated.

Second, I haven't really studied Steve Flynn's idea about going to the private sector or going elsewhere to get a bonded third party with appropriate background checks to do some of the validations. That approach might hold some promise. I would need to study it a little bit, but those kinds of auditing models are available elsewhere in government.

But I am not comfortable in saying that a cargo container can move from a high-risk designation to a low-risk designation simply because the importer filled out the paperwork correctly and we don't have any noncompliance history in our data files. I don't know if that is enough in this day and age.

Senator COLEMAN. Commander Flynn.

Commander FLYNN. I would agree with that. I just would point to the Port State Control Regime that the Coast Guard uses. The way you close the gap is you bring third parties who have expertise in the supply chains, which Customs has very little of. That is not a skill set that is a result of being a Customs official. They are trying to build it now. Instead of hiring a lot of new government employees on this front, you build that set for oversight purposes, but you go out to the marketplace and you say to the importers, as a

part of being C–TPAT, you have to have a third-party player who has verified your compliance.

Port State Control works this way. If you are an oil tanker coming into the U.S. waters, you have to have on file with the Coast Guard a certificate of financial responsibility, insurance, that you have come in. In order to get the insurance, you have to have a Classification Society go on board and confirm that you live up to the international safety standards. Then the Coast Guard spot checks when the ship comes in to say, are you living up to—have you, based on its expertise—was that inspection done with due diligence? If it was not, the ship is held up. But every other ship that used that classifier is also held up. That creates the incentive for everybody to go to the top-shelf certifier.

So there are ways in which the market can be used for expertise and to validate. Now, clearly when it is a security validation or a safety one, you need some liability protection, and that is why there will have to be a robust oversight process for this, as well.

But the only way to close the gap, I would argue, would be to take this third-party model. Otherwise, it will be years and years and as far as we can go.

Senator COLEMAN. And Mr. Stana, on behalf of the requestors of your work, Chairman Collins, Senator Lieberman, myself, and Senator Levin, I would ask you, and we will put this in writing, but continue to follow up on this. I think this is very important work, and I think we have made a lot of progress.

And again, from the beginning, I have mentioned that we need to applaud the efforts that have been taken. These are steps in the right direction. My concern, though, is that there are still significant vulnerabilities, and even in regard to issues like validation and certification, I am not sure that we are speaking the same language here. I think we have to be speaking the same language so that we can have some consistent levels of confidence that we are catching the problem before it ultimately is a huge disaster.

I also noticed that Gene Aloise, the Director at GAO, who led the team that produced the Megaports report is here and I want to thank Gene for his efforts, and again, your entire team.

I am going to keep the record open for 2 weeks. There is additional information that we want. I want to thank everybody for their testimony. This has been a very productive and very informative hearing.

With that, this hearing is adjourned.

[Whereupon, at 12:22 p.m., the Subcommittee was adjourned.]

APPENDIX

Statement of Robert C. Bonner
Commissioner
U.S. Customs and Border Protection

Hearing before the Permanent Subcommittee on Investigations, Senate Committee on Homeland Security and Governmental Affairs.

May 26, 2005

I. Introduction and Overview

Chairman Coleman, Ranking Member Levin, Members of the Subcommittee, it is a privilege to appear before you today to discuss two U.S. Customs and Border Protection (CBP) programs that are fundamental to our anti-terrorism strategy.

CBP, as the guardian of the Nation's borders, safeguards the homeland—foremost, by protecting the American public against terrorists and the instruments of terror; while at the same time, enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws. In FY 2004, CBP processed almost 30 million trade entries, collected $27 billion in revenue, seized 2.2 million pounds of narcotics, processed 428 million pedestrians and passengers, 121 million privately owned vehicles, and processed and cleared 23.5 million sea, rail and truck containers. We cannot protect against the entry of terrorists and the instruments of terror without performing all missions.

We must perform all missions without stifling the flow of legitimate trade and travel that is so important to our nation's economy. We have "twin goals:" Building more secure and more efficient borders.

II. Meeting Our Twin Goals: Building More Secure and More Efficient Borders

As the single, unified border agency of the United States, CBP's missions are extraordinarily important to the protection of America and the American people. In the aftermath of the terrorist attacks of September 11th, CBP has developed initiatives to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. Our homeland strategy to secure and facilitate cargo moving to the United States is a layered defense approach built upon interrelated initiatives. They are: the 24-Hour and Trade Act rules, the Automated Targeting System (ATS), housed in CBP's National Targeting Center, the Container Security Initiative (CSI), and the Customs-

Trade Partnership Against Terrorism (C-TPAT). My remarks will focus primarily on CSI and C-TPAT.

Advance Electronic Information

As a result of the 24-Hour rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air, and sea, so that we know who and what is coming before it arrives in the United States.

Automated Targeting System

The Automated Targeting System, which is used by National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

Extending our Zone of Security Outward– Partnering with Other Countries

Container Security Initiative (CSI)

Every day, approximately 25,000 seagoing containers arrive at our nation's seaports equating to nearly 9.2 million a year. About 90% of the world's manufactured goods move by container, much of it stacked many stories high on huge transport ships. Each year, two hundred million cargo containers are transported between the world's seaports, constituting the most critical component of global trade.

All trading nations depend on containerized shipping. Of all incoming trade to the United States, nearly half arrives by ship, and most of that is in sea containers. Other countries are even more dependent on sea container traffic, such as the U.K., Japan and Singapore.

The fact is that, today, the greatest threat we face to global maritime security is the potential for terrorists to use the international maritime system to smuggle terrorist weapons – or even terrorist operatives – into a targeted country.

If even a single container were to be exploited by terrorists, the disruption to trade and national economies would be enormous. In May 2002, the Brookings

Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could amount to $1 trillion from the resulting economic slump and changes in our ability to trade.

Clearly, the risk to international maritime cargo demands a robust security strategy that can identify, prevent and deter threats, at the earliest point in the international supply chain, before arrival at the seaports of the targeted country. We must have a cohesive national cargo security strategy that better protects us against the threat posed by global terrorism without choking off the flow of legitimate trade, so important to our economic security, to our economy, and, to the global economy.

Our nation developed a cargo security strategy that addresses cargo moving from areas outside of the United States to our ports of entry. Our strategy focuses on stopping any shipment by terrorists before it reaches the United States, and only as a last resort, when it arrives at a port of entry.

The Container Security Initiative enables the U.S. Customs and Border Protection to work with our host counterparts to screen and inspect high-risk containers before they are loaded on board vessels to the United States.

CBP implemented CSI in January 2002 because we recognized that inspecting containers with terrorist weapons concealed inside them, on arrival in the United States, would be too late. Today, CSI is one of the few multinational programs in the world actually protecting the primary means of global trade – containerized shipping – from being exploited or disrupted by international terrorists. CSI adds security to the movement of maritime cargo containers, and it allows containers to move faster, more efficiently and predictably through the supply chain.

The four core elements of CSI are:

- Identifying high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
- Prescreening containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- Using technology to prescreen high-risk containers including large-scale X-ray and gamma ray machines and radiation detection devices.
- Using smarter, more secure containers. This allows CBP officers at United States ports of arrival to identify containers that have been tampered with during transit.

Through the CSI program, CBP deploys multi-disciplined teams, including agents, intelligence analysts and customs officers to selected foreign seaports throughout the world, to protect the United States and its citizens from both direct and indirect terrorist attacks in the maritime cargo environment. Operating procedures for CSI ports are governed by Declaration of Principles and agreed upon operating

procedures, in which the host government commits to pre-screen containers that pose a risk for terrorism.

Today, CSI is operational in 36 ports in Europe, Asia, Africa and North America. CBP is working towards strategically locating CSI in additional areas of the world where terrorists have a presence.

CBP will continue expanding the CSI security network by using advanced technologies while optimizing resources such as the National Targeting Center as a communications hub coordinating domestic and international communication. Through a framework for security and facilitation of global trade, endorsed by the World Customs Organization, CBP intends to strengthen trade data and targeting by promoting harmonized standards for data elements, examinations and risk assessments.

To inspect all high-risk containers before they are loaded on board vessels to the United States, CBP plans to continue fostering partnerships with other countries and our trading partners. In addition, the World Customs Organization, the European Union and the G8 support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world

In providing security for the maritime transportation system, we intend to ensure that the greater security does not slow down or choke off the flow of trade. The CSI program secures and facilitates the movement of legitimate trade by effectively using the time prior to the lading of the container for inspections.

Extending our Zone of Security – Partnering with the Trade

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary partnership between CBP and industry to secure the international supply chain. C-TPAT importers secure supply chains from the foreign factory loading docks of their vendors to the port of arrival in the U.S. CBP, in return, offers C-TPAT shipments expedited processing and provides C-TPAT participants with other benefits.

To join C-TPAT, a company must conduct a comprehensive self-assessment of its current supply chain security procedures using C-TPAT security criteria and best practices developed in partnership with the trade. A participant must also commit to increasing its supply chain security to meet minimal supply chain security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chains to ensure that those businesses also increase their supply chain security. By leveraging the influence of importers, C-TPAT is able to increase security of U.S. bound goods to the point of origin (i.e., to the point of container stuffing). This reach -- to the foreign loading dock –is

beyond the regulatory reach of the U.S. Government, but critical to the goal of increasing supply chain security.

C-TPAT is currently open to all importers, cross-border air, sea, truck, and rail carriers, brokers, freight forwarders, consolidators, non-vessel operating common carriers, and U.S. Marine and Terminal operators. We are currently enrolling certain foreign manufacturers in the C-TPAT program and will continue to develop ways to include this important element of the supply chain in the program. The intent is to increase point of origin to point of arrival security into the supply chain.

Although C-TPAT is a partnership, the risk is too great to simply take participants at their word when it comes to their supply chain security. We have created a cadre of specially trained supply chain security specialists to validate the commitments made by C-TPAT participants – to ensure that they are increasing supply chain security as they have promised CBP, and that their measures are reliable and effective. These specialists meet with personnel from C-TPAT certified companies and their business partners and observe the security of their supply chains, including security at overseas loading docks and manufacturing plants, as well as transportation links outbound to the U.S. Through this validation process, we work with certified members to identify ways that they can further increase their supply chain security. Companies that are not honoring their commitments may be suspended or removed from the program, and lose their C-TPAT benefits.

As of May 17, 2005, C-TPAT has assessed and accepted the security profiles of 5,013 companies; there are more than 4,200 company profiles in various stages of the application and review process. We have completed 591 validations, with an additional 2,079 validations underway or in the process of being completed.

C-TPAT Validations

Initially, CBP stated that all C-TPAT members would be 'validated' within three years of acceptance into the program. Through a validation, information provided by the C-TPAT member is verified, and recommendations are made concerning areas that require strengthening. Members who demonstrate a commitment to strengthening their supply chains receive tangible benefits from CBP. After completing several hundred validations, CBP has since modified the C-TPAT validation strategy.

After three years, it became evident that not all C-TPAT enrollment sectors exhibit the same risk to the international supply chain, nor do they possess the same ability to strengthen their supply chains throughout all components of their international supply chains. For example, U.S. based customs brokers have minimal ability to ensure sufficient supply chain security at the foreign place of stuffing, compared to U.S. based importers who have strong business influence over a foreign manufacturer or supplier. Accordingly, the enrollment sectors with the greatest ability to leverage their corporate strength and demand more security enhancements from foreign entities are the importers, and to a lesser extent, the carriers. Importers also receive the greatest

benefits in terms of reduced inspections. Therefore, C-TPAT validations are most effective when focused on these two enrollment sectors.

It has been demonstrated that not all supply chain components contain the same risk, especially for infiltration or exploitation by terrorist elements. A foreign manufacturer in one area of the world may be considered higher risk than a similar facility in another part of the world. Validations must focus on the highest risk component of the international supply chain.

Customs and Border Protection initiates validations based on risk, using a quantitative risk assessment tool to identify certified members with high-risk supply chains. CBP's new validation objective identifies and validates high-risk supply chain components, while engaging C-TPAT members with the greatest leverage over their foreign components of the international supply chain. This refined validation objective allows CBP to direct resources accordingly, where they can have the most impact in meeting the overall objectives of the C-TPAT program.

Customs and Border Protection uses a validation selection methodology that relies upon quantifiable data coupled with an objective assessment of the submitted security profile to determine the top priorities for validations. In particular, CBP is now placing emphasis on the importer and carrier sectors, and has modified its validation approach to maximize resources and increase efficiencies, such as validating multiple foreign suppliers within a geographic proximity. CBP has also enhanced its ability to record and measure validation results by developing the Automated Validation Assessment Tool, which is an electronic questionnaire that automatically scores and weighs the findings of the Supply Chain Specialist to produce an overall assessment of the supply chain security measures in place. Validation site visits are also documented in validation reports that contain sections on Findings, Recommendations and Best Practices. Identified weaknesses must be corrected in order for the member to retain benefits.

Foreign Site Visits

The member's C-TPAT point of contact and the CBP Supply Chain Specialists work together to arrange the logistics involved for the foreign site visit. Typically, the point of contact or an individual who was in attendance at the domestic corporate meeting also attends the foreign site validation visit.

Foreign site visits usually include a corporate meeting with foreign manufacturer corporate personnel, and a tour of the appropriate manufacturing, shipping, consolidation and port facilities.

Minimum Security Criteria for Importers

As the Customs-Trade Partnership Against Terrorism has evolved, we have steadily added to the rigor of the program. We must continue to work to close the gaps that a global terrorist might seek to exploit. From the beginning, voluntary participation and jointly developed security criteria, best practices, and implementation procedures were the guiding principles for C-TPAT. As the program has grown, so has our need for more clearly defined security criteria to establish the minimum, baseline security expectations for membership in this voluntary, incentives-based program.

In late October 2004, in discussions with the trade community, we began drafting more clearly defined, minimum-security criteria for importers wishing to participate in the C-TPAT program. After months of constructive dialogue, we developed minimum security criteria designed to accomplish two important goals: first, to offer flexibility to accommodate the diverse business models represented within the international supply chain; and second, to achieve CBP's twin goals of security and facilitation.

The minimum security criteria for importers became effective on March 25, 2005. Importers who have not yet joined the C-TPAT program must meet or exceed these security criteria before being certified and eligible for program benefits. For current C-TPAT members, implementation is being phased in to ensure that an importer's security measures are consistent with these security criteria.

First, importers were given 60 days from the date of the announcement to meet the container security, physical security, and physical access controls outlined in the new security criteria. These security elements will provide an immediate 'hardening' of the physical supply chain.

Second, within 120 days — or by July 26, 2005 — C-TPAT members will be expected to address internal or procedural security elements, including personnel security, procedural security, information technology security, and the establishment of a security training and threat awareness program. These security measures will help strengthen overall supply chain management practices.

Third, importers will have 180 days — or until September 26, 2005 — to leverage their corporate strength to push security enhancements back into their supply chain, from point of stuffing to point of arrival and the CBP clearance process. These business partner requirements outlined in the security criteria are paramount to an effective supply chain security program.

Customs and Border Protection plans to clearly define the minimum security criteria for each enrollment sector shortly.

Benefits for Certified Members

Customs-Trade Partnership Against Terrorism certified members that initiate actions that further secure their supply chain receive benefits from CBP. They include

reduced enforcement and compliance inspections and expedited clearance times, eligibility to participate in CBP programs such as the Free and Secure Trade program (FAST) and the Importer Self Assessment, as well as access to CBP training seminars open only to certified members.

C-TPAT members also benefit from the increased supply chain security by realizing more efficient supply chains, improved use of assets, reduced costs, revenue growth, and reduced pilferage.

Companies that do more to secure their supply chains, those that go above and beyond the minimal requirements, should be recognized. CBP has implemented a tiered system of C-TPAT benefits, based on the level of security, validation results, and use of C-TPAT best practices.

Tier I consists of certified companies who receive the benefits reduced ATS scoring, and the other benefits of a certified C-TPAT member. These are the companies that have submitted their security plans, committed to meet C-TPAT minimal security criteria, had those plans approved by CBP supply chain security specialists, and, based upon vetting, have had no history of significant compliance or law enforcement problems.

Tier II consists of validated C-TPAT companies. They would get a further ATS reduction in their scoring, and even fewer inspections. CBP has validated the supply chains of 12 percent of all certified partners, and another 40 percent are in the process. We are aggressively recruiting permanent Supply Chain Specialists and will increase dramatically the number of people we have conducting validations, and the number of validations completed.

Tier III is CBP's vision for the highest level of C-TPAT. Tier III would consist of those fully certified, validated C-TPAT partners who exceed the minimum standards, and have adopted C-TPAT best practices; for example, those that use C-TPAT container security devices such as the Smart Box. Certified, validated C-TPAT importers using C-TPAT best security practices---will be subject to relatively infrequent random inspections.

CBP's goal is a more secure supply chain that includes point of origin security, security at point of stuffing, ensured by C-TPAT validated partners who control their supply chain and assure point of origin security, who use a smart container, or see that their foreign vendors do, and who ship their goods through a CSI port to the United States.

Among the added benefits for validated C-TPAT partners will be moving the shipments of C-TPAT members to the front of the inspection line, when a shipment does need to go to secondary, either for a random inspection or due to other agency requirements. Demonstrated investments to meet and maintain best practices should be recognized and also rewarded.

Performance Measures

Measuring program effectiveness in terms of "deterrence" is complicated. And, although traditional workload measures are a valuable indicator of the challenges CBP faces, they do not necessarily reflect the success or failure of the agency's efforts. The direct impact being made on unlawful activity is often unknown. Because of these and other unidentified variables, the traditional economics and approaches used to measure performance can be challenging.

The Customs-Trade Partnership Against Terrorism program recognizes the need for effective measures to determine the success of the program. While new measures are under development, C-TPAT currently uses three measures to determine the scope of the C-TPAT program. These measures help gauge the success of C-TPAT partnership efforts. They include the percent of sea container cargo transported by C-TPAT carriers, the percent of value imported by C-TPAT importers, and the percent of C-TPAT importer entry volume.

In addition, reduced cargo inspections are a benefit importers receive for joining C-TPAT. To determine if members receive reduced inspections, a ratio of targeted inspections of C-TPAT shipments versus non C-TPAT shipments is calculated. Since C-TPAT benefits include reduced compliance inspections, the ratio of C-TPAT entry inspection compared to non-C-TPAT entry inspections is also calculated.

Finally, validations demonstrate and confirm the effectiveness, efficiency and accuracy of a C-TPAT certified member's supply chain security. Validation report results are used to determine the ratio of recommendations included in the report.

Recruitment of Permanent Supply Chain Specialists

In FY04, CBP created the Supply Chain Specialist position, to assist with key program elements. The SCS serves as the principal advisor and primary point of contact for certified members in the C-TPAT program. The Supply Chain Specialist is a Headquarters position strategically located in four field offices (NY, Miami, Los Angeles, and Washington, DC) to better facilitate C-TPAT validations, various anti-terrorism / anti-smuggling training and awareness programs and provide general overall program guidance.

CBP continues to recruit permanent Supply Chain Specialists from within the government and from the private sector, and has trained 38 field officers to help assist in the initiation of validations. As of May 17, 2005, there are 66 permanent Supply Chain Specialists on board, with an additional four waiting to report. CBP anticipates having 100 Supply Chain Specialists on board by the end of FY05, which will enable the C-TPAT program to substantially increase the number of validations performed.

Government Accountability Office Recommendations

Over the last several months, CBP has made substantial progress in areas of the Government Accountability Office recommendations.

In particular, the C-TPAT program has strengthened the validation process as described above, employing an effective validation selection methodology, modifying its validation approach to maximize resources and increase efficiencies, and enhancing its ability to record and measure validation results.

In addition, CBP has published the C-TPAT Strategic Plan, clearly articulating program goals and strategies, and completed the C-TPAT Human Capital Plan, which addresses recruitment, training and workload issues.

With regard to the need for performance measures, Customs and Border Protection has provided quantifiable workload measures. Gauging deterrence and prevention remain a very challenging task. We will continue our efforts in this area.

Finally, steps have been taken to automate key processes, and implement a records management system to document key decisions and operational events, including decisions made through the validation process, and tracking member status.

In three years, C-TPAT has successfully increased supply chain security through the voluntary enrollment and private sector enhancement of supply chain security.

As a result of thousands of C-TPAT participants voluntarily sharing with the government details of sensitive corporate security plans, and taking concrete steps to improve their security procedures, Customs and Border Protection has gained increased confidence in the efforts of this government-private sector partnership to increase supply chain security Given the global nature of the supply chain and the inherent difficulty of regulating overseas activity, private sector participation has been critical to increasing supply chain security. Based upon this experience, CBP believes that C-TPAT companies pose a low risk for terrorism. Notwithstanding this determination, C-TPAT members are not exempt from CBP security protocols, such as advance reporting requirements, enforcement and security inspections, random inspections, and non-intrusive screening technology such as radiation portals. In addition, CBP has developed a risk-based approach to validate the security enhancements that C-TPAT members have committed to achieve.

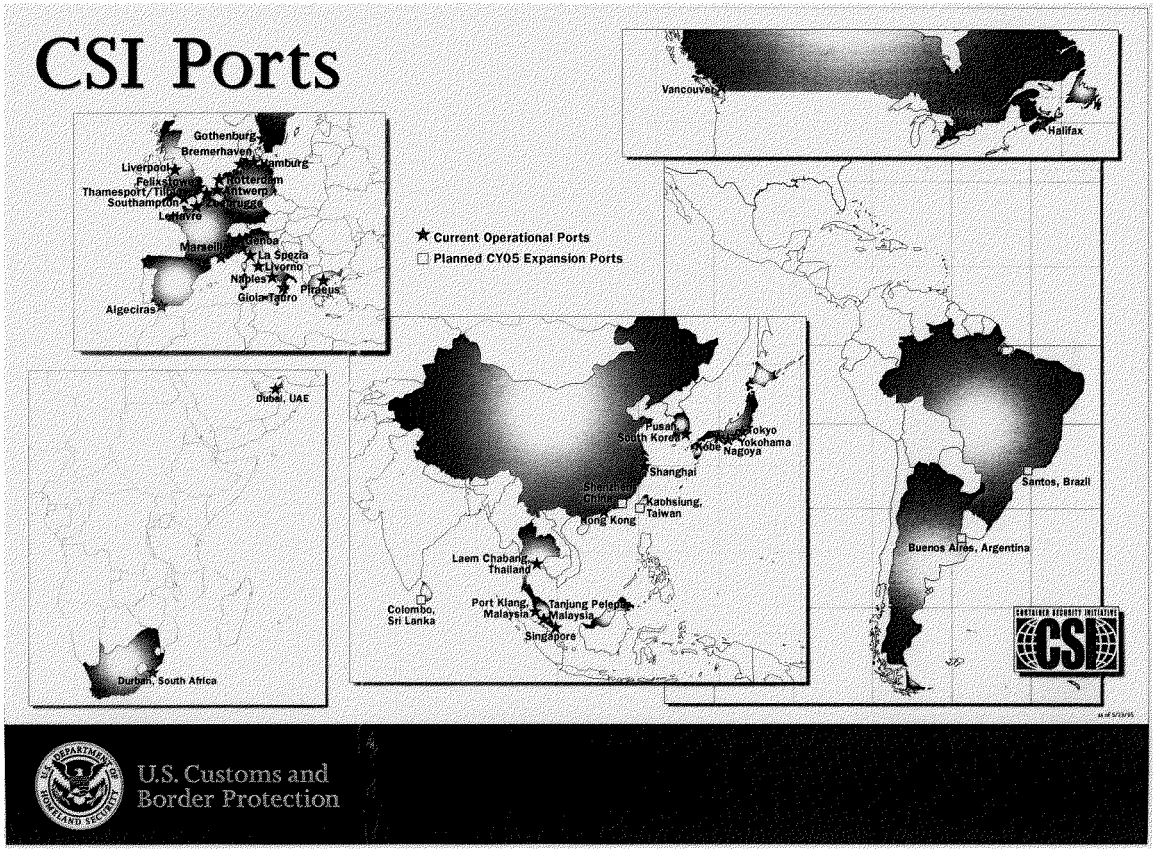
Today, C-TPAT covers about 43% of containerized imported goods into the United States, by value, a clear indication of industry's commitment to partnership, and the core principles of the program. As a requirement for doing business, many C-TPAT members require their service providers and vendors to participate in and/or adhere to C-TPAT security guidelines.

The Customs-Trade Partnership Against Terrorism program is a vital part of CBP's larger strategy – an extended border strategy designed to protect the global supply chain, our country, our economy, and ultimately the global economy. As the C-TPAT program continues to evolve, we will continue our dialogue with the trade community and continue working in a proactive, positive way to improve supply chain security and the security of global trade.

III. Conclusion

Mr. Chairman, Members of the Subcommittee, I have addressed two of CBP's critical initiatives today that will help CBP protect America against terrorists and the instruments of terror, while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. With the continued support of the President, DHS, and the Congress, CBP will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate shipments and travelers.

Thank you again for this opportunity to testify. I will be happy to answer any of your questions.



U.S. Customs and
Border Protection

CSI Ports

★ Current Operational Ports (36)

EUROPE

Algeciras, Spain
Antwerp, Belgium
Bremerhaven, Germany
Felixstowe, UK
Genoa, Italy
Gioia Tauro, Italy
Gothenburg, Sweden
Hamburg, Germany
La Spezia, Italy
Le Havre, France
Liverpool, UK
Livorno, Italy
Marseille, France
Naples, Italy
Piraeus, Greece
Rotterdam, Netherlands
Southampton, UK
Thamesport, UK
Tilbury, UK
Zeebrugge, Belgium

ASIA

Dubai, United Arab Emirates
Hong Kong
Kobe, Japan
Laem Chabang, Thailand
Nagoya, Japan
Port Klang, Malaysia
Pusan, Korea
Shanghai, People's Republic of China
Singapore, Singapore
Tanjung Pelepas, Malaysia
Tokyo, Japan
Yokohama, Japan

AFRICA

Durban, South Africa

CANADA

Halifax, Canada
Montreal, Canada
Vancouver, Canada

☐ Planned CY05 Expansion Ports

ASIA

Colombo, Sri Lanka
Kaohsiung, Taiwan
Shenzhen, People's Republic of China

LATIN AMERICA

Buenos Aires, Argentina
Santos, Brazil

U.S. Customs and Border Protection

United States Government Accountability Office

GAO

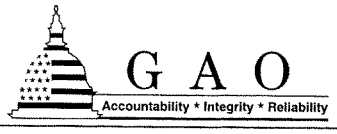
Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate

For Release on Delivery
Expected at 9:30 a.m. EDT
Thursday, May 26, 2005

HOMELAND SECURITY

Key Cargo Security Programs Can Be Improved

Statement of Richard M. Stana, Director,
Homeland Security and Justice Issues



GAO-05-466T

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-05-466T, a testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U. S. ted States Senate

Why GAO Did This Study

U.S. Customs and Border Protection (CBP) has in place two programs to help address the threat posed by terrorists smuggling weapons of mass destruction (WMD) into the United States: the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI). In July 2003, GAO reported that these programs had management challenges that limited their effectiveness. Given plans to expand both programs, in two recently issued reports GAO examined selected aspects of both programs' operations. This statement is a summary of those publicly available reports.

What GAO Recommends

For the C-TPAT program, GAO recommended that CBP eliminate the weaknesses in its validation process, complete its human capital plan and performance measures, and put in place internal controls for the program. For the CSI program, GAO recommended that CBP refine its staffing model to help improve targeting of shipments at CSI ports, develop minimum technical requirements for the capabilities of inspection equipment, and complete development of program measures.

CBP generally concurred with the recommendations and described corrective actions to respond to them.

www.gao.gov/cgi-bin/getrpt?GAO-05-466T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Rich Stana at (202) 512-8777or stanar@gao.gov.

April 26

HOMELAND SECURITY

Key Cargo Security Programs Can Be Improved

What GAO Found

In return for committing to making improvements to the security of their shipments, C-TPAT members receive a range of benefits that may change the risk characterization of their shipments, thereby reducing the probability of extensive inspection. Before providing benefits, CBP reviews the self-reported information contained in applicants' membership agreements and security profiles. Also, CBP assesses the compliance history of importers before granting them benefits. However, CBP grants benefits before members undergo the validation process, which is CBP's method to verify that their security measures are reliable, accurate, and effective. Although CBP's goal was to validate members within 3 years, to date it has validated 11 percent of them. Further, the validation process is not rigorous, as the objectives, scope, and methodology of validations are jointly agreed upon with the member, and CBP has no written guidelines to indicate what scope of effort is adequate for the validation. Also, although CBP has recently moved to a risk-based approach to selecting members for validation, it has not determined the number and types of validations that are needed to manage security risks or the CBP staff required to complete them. Further, CBP has not developed a comprehensive set of performance measures for the program, and key program decisions are not always documented and programmatic information is not updated regularly or accurately.

The CSI program is designed to target and inspect high-risk cargo containers at foreign ports before they leave for the United States. It has resulted in improved information sharing between U.S. and foreign customs operations and a heightened level of international awareness regarding securing the global shipping system. Yet, several factors limit CBP's ability to successfully target containers to determine if they are high-risk. One factor is staffing imbalances, caused by political and practical considerations, which impede CBP's targeting efforts at CSI ports. As a result, 35 percent of U.S.-bound shipments from CSI ports were not targeted and not subject to inspection overseas—the key goal of the CSI program. In addition, as of September 11, 2004, 28 percent of the containers referred to host governments for inspection were not inspected overseas for various reasons such as operational limitations. One percent of these referrals were denied by host government officials, generally because they believed the referrals were based on factors not related to security threats. For the 72 percent of referred containers that were inspected overseas, CBP officials told us that no WMD were discovered. However, the nonintrusive inspection equipment used at CSI ports varies in detection capability, and there are no minimum technical requirements for equipment used as part of CSI. As a result, CBP has limited assurance that inspections conducted under CSI are effective at detecting and identifying terrorist WMD in containers. Finally, CBP continues to make refinements to the strategic plan and performance measures needed to help manage the program and achieve program goals. Until these refinements are completed, it will be difficult to assess progress made in CSI operations.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to provide a summary of our recent reports for you on the Department of Homeland Security's (DHS) programs to improve the security of the international supply chain, as well as target oceangoing cargo containers for inspection at foreign seaports before they arrive at destinations in the United States.

In the aftermath of the terrorist attacks of September 11, 2001, there is heightened concern that terrorists may try to smuggle weapons of mass destruction (WMD) into the United States, specifically by using one of the millions of cargo containers that arrive at our nation's seaports each year. If terrorists did so and detonated such a weapon (e.g., a radiological explosive device) at a seaport, the incident could cause widespread death and damage to the immediate area, perhaps shut down seaports nationwide, cost the U.S. economy billions of dollars, and seriously hamper international trade.

DHS and its U.S. Customs and Border Protection (CBP) are responsible for addressing the threat posed by terrorists smuggling weapons into the United States. To carry out this responsibility, CBP has in place programs known as the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI). The C-TPAT program attempts to improve the security of the international supply chain (flow of goods from manufacturer to retailer). It is a cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected. C-TPAT membership is open to U.S.- and foreign-based companies whose goods are shipped to the United States via air, rail, ocean, and truck carriers. The CSI program specifically addresses the security of oceangoing cargo containers. Under the program, CBP places staff at foreign seaports to work with foreign counterparts to use risk assessment information to select, or target, those containers at risk of containing WMD and inspect them before they are shipped to the United States.

This statement presents a summary of our latest efforts in a series of GAO reports that evaluate CBP's response to the terrorist threat.[1] As requested,

[1] A list of related GAO reports appears at the end of this statement.

my testimony will focus on our assessment of CBP's efforts under both C-TPAT and CSI. Regarding C-TPAT, I will address the following issues:

- What benefits does CBP provide to C-TPAT members?
- Before providing benefits, what approach does CBP take to determine C-TPAT members' eligibility for them?
- After providing benefits, how does CBP verify that members have implemented their security measures?
- To what extent has CBP developed strategies and related management tools for achieving the program's goals?

Regarding CSI, I will address the following issues:

- What factors affect CBP's ability to target shipments at overseas seaports?
- Under CSI, to what extent have high-risk containers been inspected overseas prior to their arrival at U.S. destinations?
- To what extent has CBP developed strategies and related management tools for achieving the program's goals?

My statement today represents a summary of two unrestricted reports we have provided to Congress on these programs—that is, our March 2005 report on C-TPAT[2] and our April 2005 report on CSI.[3]

Summary

C-TPAT Issues

Our report on C-TPAT noted that C-TPAT members receive a range of benefits that reduce the level of scrutiny CBP provides to their shipments

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

[3]GAO, *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).

bound for the United States. These benefits may change the risk characterization of their shipments, thereby reducing the probability of extensive documentary and physical inspection. Before providing benefits, CBP uses a two-pronged approach to assess C-TPAT members. First, CBP has a certification process to review the self-reported information contained in applicants' membership agreements and security profiles. Second, CBP has in place a vetting process to try to assess the compliance with customs laws and regulations and violation history of and intelligence data on importers before granting them benefits. However, CBP grants benefits to members before they undergo the validation process, which is CBP's method to verify that members' characterization of their security measures are accurate and that the security measures have been implemented.

Regarding the validation process, we found several weaknesses that compromise CBP's ability to provide an actual verification that members' supply chain security measures are accurate and are being followed. First, the validation process is not rigorous enough to ensure that the security procedures outlined in members' security profiles are reliable, accurate, and effective. For example, CBP officials told us that validations are not considered independent audits, and the objectives, scope, and methodology of validations are jointly agreed upon with the member company. Related to this, CBP has no written guidelines to indicate what scope of effort is adequate for the validation to ensure that the member's measures are reliable, accurate, and effective. Finally, CBP has not determined the extent to which validations are needed, abandoning its original goal to validate all members within 3 years because of rapid growth in membership and CBP staffing constraints. In 3 years of C-TPAT operation, CBP has validated about 11 percent of its certified members.

We also found weaknesses in some of the tools CBP uses to manage the program that could hinder achieving the program's goals. The new CBP strategic plan appears to provide the bureau with a general framework on which to base key decisions, including key strategic planning elements such as strategic goals, objectives, and strategies. CBP told us it has developed some initial performance measures to capture the program's impact but has not developed a comprehensive set of performance measures and indicators to monitor the status of program goals. Finally, the C-TPAT program lacks an effective records management system. CBP's record keeping for the program is incomplete, as key decisions are not always documented and programmatic information is not updated regularly or accurately.

Our report contained several recommendations to enhance the C-TPAT program. Specifically, we made recommendations to CBP to provide appropriate guidance to specialists conducting validations, determine the extent to which members should be validated in lieu of the original goal to validate all members within 3 years of certification, complete performance measures and a human capital plan, and implement a records management system for the program. CBP generally agreed with our recommendations and cited corrective actions the bureau either had taken or planned to take to implement them.

CSI Issues

Our report on CSI noted improved information sharing between U.S. and foreign customs operations and a heightened level of bilateral cooperation and international awareness regarding securing the whole global shipping system across governments. However, other, negative factors limit CBP's ability to successfully target containers to determine if they are high-risk. One such factor is staffing imbalances, which impede CBP from targeting all containers shipped from some CSI ports before they leave for the United States. For example, political and practical considerations have limited the number of staff at some ports. As a result of these limitations, 35 percent of U.S.-bound shipments from CSI ports were not targeted and were therefore not subject to inspection overseas—the key goal of the CSI program. We also noted that CBP's reliance on placing staff at overseas ports without considering whether some targeting functions could be performed domestically limits the program's operational efficiency and effectiveness.

Our report also noted that as of September 2004, 28 percent of the containers referred to host governments for inspection had not been inspected overseas. These containers were not inspected for reasons such as operational limitations that prevented the containers from being inspected before they left the port. One percent of these referrals were denied by host government officials, generally because they believed the referrals were based on factors not related to security threats, such as drug smuggling. For the 72 percent of referred containers that were inspected overseas, CBP officials told us that no WMD were discovered, although they acknowledged that technologies to detect other WMDs have limitations. Also, considering that the nonintrusive inspection equipment used at CSI ports varies in detection capability and that there are no minimum technical requirements for equipment used as part of CSI, CBP has limited assurance that inspections conducted under CSI are effective at detecting and identifying terrorist WMD in containers.

The bureau continues to make refinements to management tools needed to help achieve program goals. Although CBP issued a strategic plan for CSI in February 2004, the bureau continues to develop three key elements: (1) describing how performance goals are related to general goals of the program, (2) identifying key external factors that could affect program goals, and (3) describing how programs are to be evaluated. Although CBP has made progress in the development of some outcome-oriented performance measures, it continues to face challenges in developing performance measures to assess the effectiveness of CSI targeting and inspection activities. Therefore, it is difficult to assess progress made in CSI operations over time, and it is difficult to compare CSI operations across ports.

Our report made several recommendations to improve the CSI program. Specifically, we recommended that CBP revise its staffing model, develop minimum detection capability requirements for nonintrusive inspection equipment used in the program, and complete development of performance measures for all program objectives. CBP generally agreed with our recommendations and cited corrective actions the bureau either had taken or planned to take to implement them.

Background

CBP maintains two overarching goals: (1) increasing security and (2) facilitating legitimate trade and travel. Disruptions to the supply chain could have immediate and significant economic impacts. For example, in terms of containers, CBP data indicates that in 2003 about 90 percent of the world's cargo moved by container. In the United States, almost half of all incoming trade (by value) arrived by containers on board ships. Additionally, containers arrive via truck and rail. Both admitting dangerous cargo into the country and delaying the movement of cargo containers through ports of entry could negatively affect the national economy. Therefore, CBP believes it is vital to try to strike a balance between its antiterrorism efforts and facilitating the flow of legitimate international trade and travel.

Vulnerability of the Supply Chain

The terrorist events of September 11, 2001, raised concerns about company supply chains, particularly oceangoing cargo containers, potentially being used to move WMD to the United States. An extensive body of work on this subject by the Federal Bureau of Investigation and academic, think tank, and business organizations concluded that while the likelihood of such use of containers is considered low, the movement of oceangoing containerized cargo is vulnerable to some form of terrorist

action. Such action, including attempts to smuggle either fully assembled WMD or their individual components, could lead to widespread death and damage.

The supply chain is particularly vulnerable to potential terrorists because of the number of individual companies handling and moving cargo through it. To move a container from production facilities overseas to distribution points in the United States, an importer has multiple options regarding the logistical process, such as routes and the selection of freight carriers. For example, some importers might own and operate key aspects of the overseas supply chain process, such as warehousing and trucking operations. Alternatively, importers might contract with logistical service providers, including freight consolidators and nonvessel-operating common carriers. In addition, importers must choose among various modes of transportation to use, such as rail, truck, or barge, to move containers from the manufacturer's warehouse to the port of lading.

C-TPAT Is Part of CBP's Layered Enforcement Strategy

CBP has implemented a layered enforcement strategy to prevent terrorists and WMD from entering the United States through the supply chain. One key element of this strategy is the C-TPAT program. Initiated in November 2001, C-TPAT is a voluntary program designed to improve the security of the international supply chain while maintaining an efficient flow of goods. Under C-TPAT, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security. In return for committing to making improvements to the security of their shipments by joining the program, C-TPAT members may receive benefits that result in reduced scrutiny of their shipments (e.g., reduced number of inspections or shorter border wait times for their shipments). C-TPAT membership is open to U.S.-based companies in the trade community, including (1) air/rail/sea carriers, (2) border highway carriers, (3) importers, (4) licensed customs brokers, (5) air freight consolidators and ocean transportation intermediaries and nonvessel-operating common carriers, and (6) port authorities or terminal operators. Of these companies, CBP grants importers key program benefits. According to CBP, program membership has grown rapidly, and continued growth is expected, especially as member importers are requiring their suppliers to become C-TPAT members. For example, as of January 2003 approximately 1,700 companies had become C-TPAT members. By May 2003, the number had nearly doubled to 3,355. According to CBP officials, as of April 2005, the C-TPAT program had over 9,000 members. For fiscal year 2005, the C-TPAT budget request was about $38 million, with a requested budget for fiscal year 2006 of about $54 million for program expansion efforts. As of

August 2004, CBP had hired 40 supply chain specialists, who are dedicated to serve as the principal advisers and primary points of contact for C-TPAT members.[4] The specialists are located in Washington, D.C., Miami, Florida, Los Angeles, California, and New York, New York.

CBP has a multistep review process for the C-TPAT program. Applicants first submit signed C-TPAT agreements affirming their desire to participate in the voluntary program. Applicants must also submit security profiles—executive summaries of their company's existing supply chain security procedures—that follow guidelines jointly developed by CBP and the trade community. These security profiles are to summarize the applicant's current security procedures in areas such as physical security, personnel security, and education and training awareness. Next, CBP established a certification process in which it reviews the applications and profiles by comparing their contents with the security guidelines jointly developed by CBP and the industry, looking for any weaknesses or gaps in the descriptions of security procedures. Once any issues are resolved to CBP's satisfaction, CBP signs the agreement and the company is considered to be certified C-TPAT member, eligible for program benefits. However, members that are importers must first complete another review, as described below, before benefits can begin. CBP encourages all members to conduct self-assessments of their security profiles each year to determine any significant changes and to notify CBP. For example, members may be using new suppliers or new trucking companies and would need to update their security profiles to reflect these changes.

For certified importers, CBP has an additional review called the vetting process in which CBP reviews information about an importer's compliance with customs laws and regulations and violation history. Conducted concurrently with the certification process, CBP requires the vetting process for certified importers as a condition of granting them key program benefits. As part of the vetting process, CBP obtains trade compliance and intelligence information on certified importers from several data sources. If CBP gives the importer a favorable review under both the vetting process and the certification process, benefits are to begin

[4]For fiscal year 2004, CBP had authorization for 157 positions for supply chain specialists and support staff, but as of August 2004 had hired only 40 specialists. CBP officials noted that the bureau recognizes the need for additional permanent positions, and CBP planned to hire, train, and have in place an additional 30 to 50 supply chain specialists by the end of calendar year 2004.

within a few weeks. If not, benefits are not to be granted until successful completion of the validation process, as described below.

The final step in the review process is validation. CBP's stated purpose for validations is to ensure that the security measures outlined in certified members' security profiles and periodic self-assessments are reliable, accurate, and effective. In the validation process, CBP staff meet with company representatives to verify the supply chain security measures contained in the company's security profile. The validation process is designed to include visits to the company's domestic and, potentially, foreign sites. The member and CBP jointly determine which elements of the member's supply chain measures will be validated, as well as which locations will be visited. Upon completion of the validation process, CBP prepares a final validation report it presents to the company that identifies any areas that need improvement and suggested corrective actions, as well as a determination if program benefits are still warranted for the member.

CSI Is Another Layer of CBP's Enforcement Strategy

Announced in January 2002, the CSI program was implemented to allow CBP officials to target containers at foreign seaports so that any high-risk containers may be inspected prior to their departure for U.S. destinations. Strategic objectives for the CSI program include (1) pushing the United States' zone of security beyond its physical borders to deter and combat the threat of terrorism; (2) targeting shipments for potential terrorists and terrorist weapons, through advanced and enhanced information and intelligence collection and analysis, and preventing those shipments from entering the United States; (3) enhancing homeland and border security while facilitating growth and economic development within the international trade community; and (4) utilizing available technologies to leverage resources and to conduct examinations of all containers posing a high risk for terrorist-related activity.

To participate in the CSI program, a host nation must utilize (1) a seaport that has regular, direct, and substantial container traffic to ports in the United States; (2) customs staff with the authority and capability to inspect cargo originating in or transiting through its country; and (3) nonintrusive inspection equipment. In addition, a host nation must meet several operational criteria, including a commitment to establishing an automated risk management system. To implement the CSI program, CBP negotiates and enters into bilateral arrangements with foreign governments, specifying the placement of CBP officials at foreign ports and the exchange of information between CBP and foreign customs administrations. CBP first solicited the participation of the 20 foreign ports

that shipped the highest volume of ocean containers to the United States. These top 20 ports are located in 14 countries and regions and shipped a total of 66 percent of all containers that arrived in U.S. seaports in 2001. CBP has since expanded CSI to strategic ports, which may ship lesser amounts of cargo to the United States but may also have terrorism or geographical concerns. As shown in table 1, as of February 2005, CSI was operational at 34 ports, located in 17 countries or regions. For fiscal year 2005, the CSI budget was about $126 million, with a budget of about $139 million requested in fiscal year 2006.

Table 1: CSI Operational Seaports, as of February 2005

Country/region	CSI port	Date CSI operations began at port
Canada	Halifax	March 2002
	Montreal	March 2002
	Vancouver	February 2002
The Netherlands	Rotterdam	September 2002
France	Le Havre	December 2002
	Marseilles	January 2005
Germany	Bremerhaven	February 2003
	Hamburg	February 2003
Belgium	Antwerp	February 2003
	Zeebrugge	October 2004
Republic of Singapore	Singapore	March 2003
Japan	Yokohama	March 2003
	Tokyo	May 2004
	Nagoya	August 2004
	Kobe	August 2004
Hong Kong Special Administrative Region of China	Hong Kong	May 2003
Sweden	Gothenburg	May 2003
United Kingdom	Felixstowe	May 2003
	Liverpool	October 2004
	Southampton	October 2004
	Thamesport	October 2004
	Tilbury	October 2004
Italy	Genoa	June 2003
	La Spezia	June 2003
	Livorno	December 2004
	Naples	September 2004
	Gioia Tauro	October 2004
South Korea	Busan	August 2003
South Africa	Durban	December 2003
Malaysia	Port Klang	March 2004
	Tanjung Pelepas	August 2004
Greece	Piraeus	July 2004
Spain	Algeciras	July 2004
Thailand	Laem Chabang	August 2004

Source: CBP.

CBP then deploys a CSI team, which generally consists of three types of officials—targeters, intelligence analysts, and special agents. These officials come from either CBP or U.S. Immigration and Customs Enforcement (ICE). The team leader is a CBP officer or targeter who is assigned to serve as the immediate supervisor for all CSI team members and is responsible for coordinating with host government counterparts in the day-to-day operations. The targeters are team members responsible for targeting shipments and referring those shipments they determine are high-risk to host government officials for inspection. The targeter may also observe inspections of containers. The intelligence analyst is responsible for gathering information to support targeters in their efforts to target containers. In addition, the special agents are to coordinate all investigative activity resulting from CSI-related actions, as well as act as liaison with all appropriate U.S. embassy attachés. Under the CSI program, the targeting of cargo is largely dependent on CBP targeters' review of information contained within CBP's Automated Targeting System (ATS) in conjunction with other sources to determine the risk characterization of a container.[5]

CSI teams refer any containers they characterize as high-risk to host government officials for concurrence to inspect. If host government officials, on the basis of their review, agree that the shipment is high-risk, they will proceed with an inspection using nonintrusive inspection equipment (that is, X-ray) and physical examinations, if warranted. If the host government officials determine, on the basis of their review, that a shipment is not high-risk, they will deny inspection of the shipment. For any high-risk shipment for which an inspection is not conducted, CSI teams are to place a domestic hold on the shipment, so that it will be inspected upon arrival at its U.S. destination.

Prior GAO Work Disclosed Challenges

We have conducted previous reviews of the C-TPAT and CSI programs and CBP's targeting and inspection strategy. In July 2003, we reported that CBP's management of C-TPAT and CSI had not evolved from a short-term focus to a long-term strategic approach.[6] We recommended that the

[5]For all cargo containers arriving in the United States, CBP uses a targeting strategy that employs its computerized targeting model, the Automated Targeting System. CBP uses ATS to review container documentation and help characterize the risk level of shipments to determine the need for additional documentary review or physical inspection.

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

Secretary of Homeland Security work with the CBP Commissioner to develop for both programs (1) strategic plans that clearly lay out the program's goals, objectives, and detailed implementation strategies; (2) performance measures that include outcome-oriented indicators; and (3) human capital plans that clearly describe how the programs will recruit, train, and retain new staff to meet the program's growing demands as CBP implements new program elements. In March 2004, we testified that CBP's targeting system does not incorporate all key elements of a risk management framework and recognized modeling practices in assessing the risks posed by oceangoing cargo containers.[7]

C-TPAT Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security

My statement will now focus on the results of our work on the C-TPAT program.

C-TPAT Benefits Reduce Scrutiny of Shipments

In our C-TPAT report we noted that the C-TPAT program offers numerous benefits to C-TPAT members. As table 2 shows, these benefits may reduce the scrutiny of members' shipments. These benefits are emphasized to the trade community through direct marketing in presentations and via CBP's Web site. Although these benefits potentially reduce the likelihood of inspection of members' shipments, CBP officials noted that all shipments entering the United States are subject to random inspections by CBP officials or inspections by other agencies.

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

Table 2: Benefits for C-TPAT Members

Benefit	Reduces amount of scrutiny provided for members?
A reduced number of inspections and reduced border wait times	Yes
Reduced selection rate for trade-related compliance examinations	Yes
Self-policing and self-monitoring of security activities	Yes
Access to the expedited cargo processing at designated FAST lanes (for certified highway carriers and certified importers along the Canadian and Mexican borders, as well as for certified Mexican manufacturers)	Yes
Eligible for the Importer Self-Assessment Program and has priority access to participate in other selected customs programs (for certified importers only)	Yes
A C-TPAT supply chain specialist to serve as the CBP liaison for validations	No
Access to the C-TPAT members list	No
Eligible to attend CBP-sponsored antiterrorism training seminars	No

Source: CBP's C-TPAT Strategic Plan, January 2005.

CBP Grants Benefits before Verification of Security Procedures

We also reported that CBP does not grant program benefits until it has reviewed and certified applicants' security profiles and, for importers, completed an additional review called the vetting process. According to CBP, approximately 23 percent of the security profiles it received contained shortcomings that prevented the companies from being certified and eligible for program benefits. However, CBP has stated that a company will not be rejected from participating in C-TPAT if there are problems with its security profile. Instead, CBP says it will work with companies to try to resolve and overcome any deficiencies with the profile itself. Regarding the vetting process, we reported that according to CBP, to date most members who have been vetted have proven to have favorable or neutral importing histories. CBP officials told us that not many members have been denied benefits as a result of the vetting process.

Although CBP does not grant program benefits until it has certified and vetted members, we reported that neither the certification nor the vetting process provides an actual verification that the supply chain security measures contained in the C-TPAT member's security profile are accurate and are being followed before CBP grants the member benefits. A direct

examination of selected members' security procedures is conducted later as part of CBP's validation process, as discussed below.

Weaknesses Exist in Process for Verifying Security Procedures

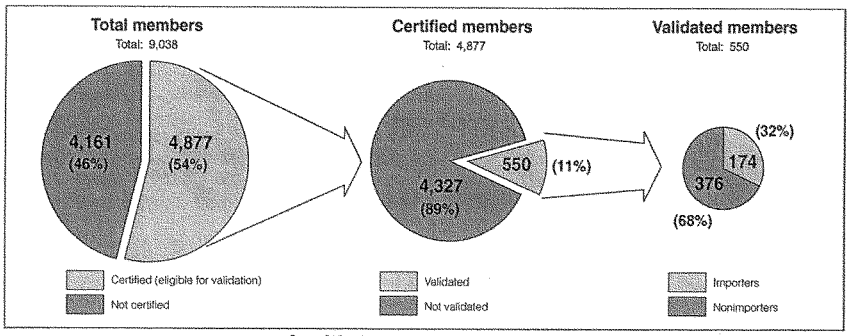
As we reported, we found weaknesses in the validation process that limit CBP's ability to ensure that the C-TPAT program supports the prevention of terrorists and terrorist weapons from entering the United States. First, we reported that CBP's validation process is not rigorous enough to achieve its stated purpose, which is to ensure that the security procedures outlined in members' security profiles are reliable, accurate, and effective. CBP officials told us that validations are not considered independent audits, and the objectives, scope, and methodology of validations are jointly agreed upon with the member representatives. In addition, CBP has indicated that it does not intend for the validation process to be an exhaustive review of every security measure at each originating location; rather, it selects specific facets of the members' security profiles to review for their reliability, accuracy, and effectiveness. For example, the guidance to ocean carriers for preparing a security profile directs the carriers to address, at a minimum, three broad areas (security program, personnel security, and service provider requirements), which contain several more specific security measures, such as facilities security and pre-employment screening. According to CBP officials, as well as our review of selected case files, validations examine only a few facets of members' security profiles. CBP supply chain specialists, who are responsible for conducting most of the validations, are supposed to individually determine which segments of a company's supply chain security will be suggested to the member for validation. To assist in this decision, supply chain specialists are supposed to compare a company's security profile, as well as any self-assessments or other company materials or information retrievable in national databases, against the C-TPAT security guidelines to determine which elements of the profile will be validated. Once the supply chain specialist determines the level and focus of the validation, the specialist is supposed to contact the member company with a potential agenda for the validation. The two parties then jointly reach agreement on which security elements will be reviewed and which locations will be visited.

Moreover, as we reported, CBP has no written guidelines for its supply chain specialist to indicate what scope of effort is adequate for the validation to ensure that the member's security measures are reliable, accurate, and effective, in part because it seeks to emphasize the partnership nature of the program. Importantly, CBP has no baseline standard for what minimally constitutes a validation. CBP discourages supply chain specialists from developing a set checklist of items to

address during the validation, as CBP does not want to give the appearance of conducting an audit. In addition, as discussed below, the validation reports we reviewed did not consistently document how the elements of members' security profiles were selected for validation.

Second, we also reported that CBP has not determined the extent to which it must conduct validations of members' security profiles to ensure that the operation of C-TPAT is consistent with its overall approach to managing risk. In 3 years of C-TPAT operation, CBP has validated about 11 percent of its certified members. CBP's original goal was to validate all certified members within 3 years of certification. However, CBP officials told us that because of rapid growth in program membership and its staffing constraints, it would not be possible to meet this goal. In February 2004, CBP indicated that approximately 5,700 companies had submitted signed agreements to participate in the program. As shown in figure 2, by April 2005, the number of members had grown to over 9,000, about 4,800 of which had been certified and were thus eligible for validation. According to CBP, as of April 2005, CBP staff had completed validations of 550 companies, including 174 importers.

Figure 2: Status of Validating C-TPAT Members, as of April 1, 2005



Source: GAO analysis of CBP data.

In our C-TPAT report we noted that CBP has made efforts to hire additional supply chain specialists to handle validations for the growing membership. As of August 2004, CBP had hired a total of 40 supply chain

specialists to conduct validations, with 24 field office managers also available to conduct validations. CBP officials told us the bureau is currently conducting as many validations as its resources allow. However, CBP has not determined the number of supply chain specialists it needs or the extent to which validations are needed to provide reasonable assurance that the program is consistent with a sound risk management approach to securing U.S.-bound goods.

Finally, we reported that it would not be possible for CBP to meet its goal of validating every member within 3 years of certification. Instead, CBP told us it is using a risk-based approach, which considers a variety of factors to prioritize which members should be validated as resources allow. CBP has an internal selection process it is supposed to apply to all certified members. Under this process CBP officials are supposed to prioritize members for validation based on established criteria but may also consider other factors. For example, recent seizures involving C-TPAT members can affect validation priorities. If a member is involved in a seizure, CBP officials noted that the member is supposed to lose program benefits and be given top priority for a validation. In addition, CBP officials told us that an importer that failed CBP's vetting process would also be given top priority for a validation. CBP officials have taken this approach because any importer that fails the vetting process is not supposed to receive program benefits until after successful completion of the validation process.

Incomplete Progress Made in Addressing Management Weaknesses

As we reported, CBP continues to expand the C-TPAT program without addressing management weaknesses that could hinder the bureau from achieving the program's dual goals of securing the flow of goods bound for the United States and facilitating the flow of trade. First, we reported that CBP is still developing an implementation plan to address the strategies for carrying out the program's goals and those elements required in a human capital plan. For example, CBP said it has developed new positions, training programs and materials, and a staffing plan. Further, CBP said it will continue to refine all aspects of the C-TPAT human capital plan to include headquarters personnel, additional training requirements, budget, and future personnel profiles.

Second, we reported that CBP continues developing a comprehensive set of performance measures and indicators for C-TPAT. According to CBP, developing these measures for C-TPAT, as well as other programs in the bureau, has been difficult because CBP lacks data necessary to exhibit whether a program has prevented or deterred terrorist activity. For

example, as noted in the C-TPAT strategic plan, it is difficult to measure program effectiveness in terms of deterrence because generally the direct impact on unlawful activity is unknown. The plan also notes that while traditional workload measures are a valuable indicator, they do not necessarily reflect the success or failure of the bureau's efforts. CBP is working to collect more substantive information—related to C-TPAT activities (i.e., current workflow process)—to develop its performance measures. In commenting on a draft of our report, CBP indicated it has developed initial measures for the program but will continue to develop and refine these measures to ensure program success.

Third, we reported that CBP's record keeping for the program is incomplete, as key decisions are not always documented and programmatic information is not updated regularly or accurately. Federal regulations require that bureau record-keeping procedures provide documentation to facilitate review by Congress and other authorized agencies of government. Further, standards for internal control in the federal government require that all transactions be clearly documented in a manner that is complete, accurate, and useful to managers and others involved in evaluating operations. During our review of six company files for which validations had been completed, it was not always clear what facet of the security profile was being validated and why a particular site was selected at which to conduct the validation because there was not always documentation of the decision-making process. The aspects of the security profiles covered and sites visited did not always appear to be the most relevant. For example, one validation report we reviewed for a major retailer—one that imports the vast majority of its goods from Asia—indicated that the validation team reviewed facilities in Central America. CBP officials noted that it recently revised its validation report format to better capture any justification for report recommendations and best practices identified. After reviewing eight of the more recent validation reports, we noted that there appeared to be a greater discussion related to the rationale for validating specific aspects of the security profiles. However, the related company files did not consistently contain other documentation of members' application, certification, vetting, receipt of benefits, or validation. While files contained some of these elements, they were generally not complete. In fact, most files did not usually contain anything other than copies of the member's C-TPAT agreement, security profiles, and validation report.

Further, we reported that CBP does not update programmatic information regularly or accurately. In particular, the reliability of CBP's database to track member status using key dates in the application through validation

processes is questionable. The database, which is primarily used for documentation management and workflow tracking, is not updated on a regular basis. In addition, C-TPAT management told us that earlier data entered into the database may not be accurate, and CBP has taken no systematic look at the reliability of the database. CBP officials also told us that there are no written guidelines for who should enter information into the database or how frequently the database should be updated. We made several requests over a period of weeks to review the contents of the database to analyze workload factors, including the amount of time that each step in the C-TPAT application and review process was taking. The database information that CBP ultimately provided to us was incomplete, as many of the data fields were missing or inaccurate. For example, more than 33 percent of the entries for validation date were incomplete. In addition, data on the status of companies undergoing the validation process was provided in hard copy only and included no date information. CBP officials told us that they are currently exploring other data management systems, working to develop a new, single database that would capture pertinent data, as well as developing a paperless environment for the program.

GAO Recommendations and CBP Response

Our C-TPAT report recommended that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to take the following five actions:

- strengthen the validation process by providing appropriate guidance to specialists conducting validations, including what level of review is adequate to determine whether member security practices are reliable, accurate, and effective;
- determine the extent (in terms of numbers or percentage) to which members should be validated in lieu of the original goal to validate all members within 3 years of certification;
- complete the development of performance measures, to include outcome-based measures and performance targets, to track the program's status in meeting its strategic goals;
- complete a human capital plan that clearly describes how the C-TPAT program will recruit, train, and retain sufficient staff to successfully conduct the work of the program, including reviewing security profiles, vetting, and conducting validations to mitigate program risk; and

- implement a records management system that accurately and timely documents key decisions and significant operational events, including a reliable system for (1) documenting and maintaining records of all decisions in the application through validation processes, including but not limited to documentation of the objectives, scope, methodologies, and limitations of validations, and (2) tracking member status.

In commenting on a draft of the report, CBP generally agreed with our recommendations and outlined actions it either had taken or was planning to take to implement them.

After our work was completed, CBP issued new security criteria for C-TPAT importers. Although we have not assessed the new criteria in detail, the new criteria appear to better define the minimum security expectations of importers participating in the C-TPAT program than the prior security guidelines. For example, under the prior security guidelines, all importers were to secure containers' internal and external compartments and panels. Under the new security criteria, importers are to explicitly require all containers bound for the United States to have high-security seals affixed to them. In addition, the new criteria appear to place a greater emphasis on security procedures throughout importers' supply chains than the prior guidelines. Specifically, the new criteria state that importers must have written and verifiable processes for the selection of business partners, as well as documentation of whether these business partners are either C-TPAT certified or meet the C-TPAT security criteria—requirements not found in the prior security guidelines. However, the new security criteria do not address our recommendations for improving the program and may place an even greater emphasis on the need to strengthen the validation process. According to the new criteria, importers wishing to join the C-TPAT program must submit security profiles that address the new criteria as part of the certification process. But importers who are already C-TPAT members are not required to provide any written certification that they meet the new security criteria and will not have to resubmit their security profiles. Instead, CBP will use validations to gauge whether or not these members have adopted the new security criteria. This places a greater emphasis on the need for CBP to establish guidelines for what constitutes a validation and the extent to which it must conduct validations to ensure that the C-TPAT program is consistent with its overall approach to managing risk.

Improvements Needed in CSI Targeting, Inspection and Management Efforts

My statement will now focus on the results of our work on the CSI program.

Limitations Exist in Ability to Target Containers Overseas

In our CSI report, we noted that CBP officials told us the CSI program has produced factors that contribute to CBP's ability to target shipments at overseas seaports, including improved information sharing between the CSI teams and host government officials regarding U.S.-bound shipments and a heightened level of bilateral cooperation on and international awareness of the need for securing the global shipping system. However, we found factors that may limit the program's effectiveness at some ports, including (1) staffing imbalances at CSI ports and (2) weaknesses in one source of data CBP relies upon to target shipments.

As we reported, one factor negatively affecting CBP's ability to target containers is staffing imbalances across ports. Although CBP's goal is to target all U.S.-bound containers at CSI ports before they depart for the United States, it has not been able to place enough staff at some CSI ports to do so. As a result of these imbalances, 35 percent of U.S.-bound shipments from CSI ports were not targeted and were therefore not subject to inspection overseas—the key goal of the CSI program. CBP has been unable to staff the CSI teams at the levels called for in the CSI staffing model because of diplomatic and practical considerations. However, CBP's staffing model for CSI does not consider whether some of the targeting functions could be performed in the United States. For example, the model does not consider what minimum number of targeters need to be physically located at CSI ports to carry out duties that require an overseas presence (such as coordinating with host government officials) as opposed to other duties that could be performed in the United States (such as reviewing manifests and databases). CBP has placed targeters at its National Targeting Center to assist CSI teams in targeting containers for inspection, which demonstrates that CBP does not have to rely exclusively on overseas targeters as called for in its staffing model.

Further, we reported the existence of limitations in one data source CSI teams use for targeting high-risk containers. For CSI, CBP uses manifest information as one data source to help characterize the risk level of U.S.-

bound shipments, information that may be unreliable and incomplete. Although CBP officials told us that the quality of the manifest data has improved, there is no method to routinely verify whether the manifest data accurately reflect the contents within the cargo container.

Some Containers Were Not Inspected for a Variety of Reasons

As we reported, since the implementation of CSI through September 11, 2004, 28 percent (4,013) of containers referred to host government officials for inspection were not inspected for a variety of reasons including operational limitations that prevented the containers from being inspected before they left the port. In 1 percent of these cases, host government officials denied inspections, generally because inspection requests were based on factors not related to security threats, such as drug smuggling. Containers referred to host governments for inspection by CSI teams that are not inspected overseas are supposed to be referred for inspection upon arrival at the U.S. destination port. CBP officials noted that between July 2004 and September 2004, about 93 percent of shipments referred for domestic inspection were inspected at a U.S. port. CBP officials explained that some of these shipments were not inspected domestically because inspectors at U.S. ports received additional information or entry information that lowered the risk characterization of the shipments or because the shipments remained aboard the carrier and were never offloaded at a U.S. port.

Further, we reported that for the 72 percent (10,343) of containers that were inspected overseas, CBP officials told us there were some anomalies that led to law enforcement actions but that no WMD were discovered. There are two types of radiation detection devices used at CSI ports to inspect cargo containers—radiation isotope identifier devices and radiation portal monitors—as well as various types of X-ray and gamma-ray imaging machines used at CSI ports to inspect cargo containers, each with different detection and identification capabilities. However, the inspection equipment used at CSI ports varies in detection capability, and there are no minimum requirements for the detection capability of equipment used for CSI. In addition, technologies to detect other WMD have limitations. As a result, CBP has no absolute assurance that inspections conducted under CSI are effective at detecting and identifying WMD. According to CBP officials, the bureau has not established minimum technical requirements for the nonintrusive inspection equipment or radiation detection equipment that can be used as part of CSI because of sovereignty issues, as well as restrictions that prevent CBP from endorsing a particular brand of equipment. Although CBP cannot endorse a particular brand of equipment, the bureau could still establish

general technical capability requirements for any equipment used under CSI similar to other general requirements CBP has for the program, such as the country committing to establishing an automated risk management system. Because the CSI inspection could be the only inspection of a container before it enters the interior of the United States, it is important that the nonintrusive inspection and radiation detection equipment used as part of CSI provides some level of assurance of the likelihood that the equipment could detect the presence of WMD.

CBP Has Made Progress Developing a Strategic Plan and Performance Measures for CSI, but Further Refinements Are Needed

As we reported, CBP has made some improvements in the management of CSI, but further refinements to the bureau's management tools are needed to help achieve program goals. Regarding a strategic plan for CSI, CBP developed a strategic plan in February 2004 that contained three of the six key elements the Government Performance and Results Act (GPRA) required for executive agency strategic plans but lacked (1) a description of how performance goals and measures are related to the general goals and objectives of the program, (2) an identification of key factors external to the agency and beyond its control that could affect the achievement of general goals and objectives, and (3) a description of program evaluations. We also reported that CBP told us it was revising the CSI strategic plan to address the elements we raised in the report. We noted that it appeared that the bureau's initial efforts in this area met the intent of our prior recommendation to develop a strategic plan for CSI, but we could not determine the effectiveness of further revisions to the plan without first reviewing and evaluating them.

Further, we recommended in our July 2003 report that CBP expand efforts already initiated to develop performance measures for CSI that include outcome-oriented indicators. Until recently, CBP based the performance of CSI on program outputs such as (1) the number and percentage of bills of lading reviewed, further researched, referred for inspection, and actually inspected, and (2) the number of countries and ports participating in CSI. CBP has developed 11 performance indicators for CSI, 2 of which it identified as outcome-oriented: (1) the number of foreign mitigated examinations and (2) the percentage of worldwide U.S.-destined containers processed through CSI ports. However, CSI lacks performance goals and measures for other program objectives. In commenting on a draft of our April 2005 report, DHS noted that CBP is continuing to refine existing performance measures and develop new performance measures for its program goals. For example, CBP was developing a cost efficiency measure to measure the cost of work at a port and to contribute to staffing decisions.

GAO Recommendations and CBP Response

Our CSI report recommended that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to take the following three actions:

- revise the CSI staffing model to consider (1) what functions need to be performed at CSI ports and what functions can be performed in the United States, (2) the optimum levels of staff needed at CSI ports to maximize the benefits of targeting and inspection activities in conjunction with host nation customs officials, and (3) the cost of locating targeters overseas at CSI ports instead of in the United States;
- establish minimum technical requirements for the capabilities of nonintrusive inspection equipment at CSI ports, to include imaging and radiation detection devices, that help ensure that all equipment used can detect WMD, while considering the need not to endorse certain companies and sovereignty issues with participating countries; and
- develop performance measures that include outcome-based measures and performance targets (or proxies as appropriate) to track the program's progress in meeting all of its objectives.

In commenting on a draft of the report, DHS generally agreed with our recommendations and outlined actions CBP either had taken or was planning to take to implement them.

This concludes my statement. I would now be happy to answer any questions for the subcommittee.

GAO Contacts and Staff Acknowledgments

For further information about this testimony, please contact me at (202) 512-8816. Stephen L. Caldwell, Deena D. Richart, and Kathryn E. Godfrey also made key contributions to this statement.

Related GAO Products

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

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. GAO-05-394 (Washington, D.C.: April 15, 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).

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

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

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

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO-04-1062 (Washington, D.C.: September 30, 2004).

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

Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands. GAO-04-590 (Washington, D.C.: June 16, 2004).

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

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T (Washington, D.C.: March 23, 2004).

Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information. GAO-04-319R (Washington, D.C.: December 18, 2003).

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T (Washington, D.C.: December 16, 2003).

Posthearing Questions Related to Aviation and Port Security. GAO-04-315R (Washington, D.C.: December 12, 2003).

Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. GAO-03-1083 (Washington, D.C.: September 19, 2003).

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T (Washington, D.C.: September 9, 2003).

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

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions. GAO-03-902T (Washington, D.C.: June 16, 2003).

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO-03-843 (Washington, D.C.: June 30, 2003).

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T (Washington, D.C.: April 1, 2003).

Border Security: Challenges in Implementing Border Technology. GAO-03-546T (Washington, D.C.: March 12, 2003).

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T (Washington, D.C.: October 17, 2002).

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T (Washington, D.C.: August 5, 2002).

COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

"Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative"

Written Testimony before

a hearing of the

Permanent Sub-Committee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

on

"The Container Security Initiative and the Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?"

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies

Room 562
Dirksen Senate Office Building
Washington, D.C.

9:30 a.m.
May 26, 2005

"Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI)"

by
Stephen E. Flynn
Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairman Coleman, Senator Levin, and distinguished members of the Permanent Subcommittee on Investigations. I am honored to appear before you this morning to discuss two of the Department of Homeland Security's cornerstone programs to advance container security. The stakes associated with preventing containers from being exploited as a poor man's missile are enormous. Should a terrorist organization successfully smuggle a weapon of mass destruction into the United States and detonate it on our nation's soil, untold American lives would be in jeopardy. But such an attack also would almost certainly lead U.S. officials to close U.S. ports and borders to all inbound containers until they could assess the likelihood of follow-on attacks. If that closure extended to two or three weeks it would bring the global intermodal transportation system to its knees. Since two thirds of the total value of U.S. maritime overseas trade move in containers, American manufacturers that rely upon those shipments to keep their assembly plants operating and retailers who depend upon them to keep their shelves stocked would quickly become a part of the collateral damage. All together, the cascading costs of a weeks-long shutdown in the aftermath of a WMD attack would almost certainly be in the hundreds of billions of dollars.

As I will outline below, the Government Accountability Office is largely on the mark in highlighting a number of serious shortcomings of the C-TPAT and CSI programs as they are currently operating. However, as a stepping-off point, I believe that it is appropriate to recognize and applaud the leadership of Commissioner Robert Bonner in crafting and quickly deploying these initiatives to redress what has been a longstanding vulnerability to America's security. The objectives of these programs represent both a dramatic and constructive change in the way nations and companies have approached the issue of trade and transportation security. Among the highlights are:

- <u>C-TPAT has helped to usher in a fundamental change in how most companies and customs officials view their respective roles in container security</u>.

Prior to 9/11, the relationship between customs authorities and importers and exporters was marked by both sides approaching one another with an "us-versus-them" mentality. Customs officials saw themselves engaged in the often thankless job of trying to enforce trade laws, collect revenues, and detect and intercept contraband in the face of an ambivalent and at times, antagonistic private sector. Companies were focused on optimizing their ability to move in and out of the U.S. market at the lowest possible cost with the least amount of risk of delay. Customs regulations and enforcement activities were widely perceived as barriers to that objective. Should customs inspectors discover an infraction, the typical industry response was to treat the occasional fine as the cost of doing business. Only on rare occasions would companies make the effort to change their

operations to improve their ability to comply with the rules. C-TPAT has helped to transform this "cat-and-mouse" relationship by generating a wider appreciation within the private sector that importers and exporters must be a constructive partner in bolstering supply chain security.

- CSI creates an important opportunity for detecting and intercepting potentially dangerous cargoes before they are loaded on an ocean carrier destined for a U.S. port.

Every major U.S. container port contains other critical infrastructures such as energy refineries, chemical facilities, and power plants. And all of them are close to large urban population centers. This makes the risk associated with discovering a WMD once it is inside a U.S. port (where it could potentially be remotely detonated) unacceptably high. In addition, once a container is loaded aboard a container vessel, it is almost impossible to gain access to it. Upwards of 17 containers can be stacked on top of one another on modern container ships. The space between one stack of containers and another is often as little as eight inches. This makes it practically impossible to verify that a WMD is in a container once it is at sea. Should one be detected, the vessel would have to be diverted to a remote location where the container could be unloaded. In the interim the thousands of other containers onboard that vessel would be delayed. The best way to deal with these practical challenges is to check containers before they are loaded on a U.S.-bound ocean carrier. CSI provides a way to accomplish this.

- CSI has the potential to promote greater levels of cooperation and accountability among customs agencies.

One of the greatest benefits of deploying customs agents overseas is the potential for fostering greater levels of international cooperation, promoting professionalism, and improving information sharing among customs agents. In addition, CSI helps to reverse a trend over the past few decades towards nations making only a cursory effort to monitor the exports leaving their jurisdictions. The downside of replying primarily on import inspections to enforce rules is that it makes it much harder to assign accountability when infractions are discovered. However, the emphasis on identifying and inspecting suspicious shipments before they are loaded helps to isolate the source of illicit activity and puts the host government on notice should the problem originate within their jurisdiction.

While in principle, C-TPAT and CSI provide an excellent foundation for bolstering container security, the current way these programs are being resourced and managed is largely undercutting that potential. Among the major problems are the following:

1. The voluntary nature of C-TPAT and CSI translates into it being a "trust, but don't verify" system. The benefit of facilitated access to the U.S. market is offered without validating in advance that the participants are taking sufficient measures to ensure that they will not be compromised. This is because CBP lacks the resources and the jurisdictional reach to confirm that the thousands of C-TPAT participants are carrying out the security measures contained in their application profile. Approval is provided on the

basis of having no prior negative compliance violations and the absence of information from intelligence databases that would cause concern. In short, past performance is presumed to be a predictor of future results. There is no requirement that companies update their plans at established intervals or resubmit their plans should they make changes to their supply chains. The process of validation is essentially a "spot-check" whereby CBP inspectors first notify the participant of a pending inspection and then enter into a joint negotiation of what will be covered. Even this restrictive protocol has been barely implemented because CBP has not yet been provided adequate resources to hire and train the staff to carry out the validation process for all the current C-TPAT participants and those with outstanding applications.

CSI currently suffers from a similar problem of providing membership without requiring that the host country demonstrate their ability to conduct inspections based on an established set of criteria. For instance, there are no performance-based criteria such as the existence of a training and evaluation program for inspectors, adequate maintenance of non-intrusive inspection equipment, and periodic exercises to test the capacity of the host country to detect and respond when the system alarms on suspicious material.

2. As it currently operates, C-TPAT inadvertently may be actually raising the risk of a WMD being smuggled into the United States via a participant's supply chain. This is because CBP is placing too much reliance on the capacity of legitimate companies to independently put in place adequate supply chain security measures to deter terrorist groups from exploiting those chains. At the same time, it is has excessive faith in the intelligence it is able to collect or gain access to. Finally, it's "risk-managed" approach is premised on the flawed assumption that terrorists are most likely to target companies that: (a) have been historically susceptible to organized crime and smugglers, (b) have demonstrated a weak record of customs compliance, or (c) are new commercial entities. CBP approach is summed-up by Commissioner Bonner as: "We are inspecting 100 percent of the 'right' 5-6 percent of containers that pose the greatest threat."

Unfortunately, private companies are unlikely to have in place adequate safeguards to deter a determined terrorist, armed with a WMD. This is because private security is inherently reactive; i.e., companies cannot punish violators of their rules until there is some evidence that those rules have been broken. A good chief security officer puts in place measures that allow them to detect aberrant activity once it occurs. They then conduct professional investigations to confirm any infractions of company rules or possible crimes. The results of their investigations are passed along to senior managers who impose meaningful sanctions or refer the incident to law enforcement authorities when appropriate. When these sanctions are applied, other employees who might be tempted to disobey the rules become aware of the risk of being caught, so they are deterred.

In the case of smuggling or customs fraud, traditional corporate security is generally up to the task of deterring criminals. This is because smuggling and cheating typically involve ongoing conspiracies. Few criminals have the discipline to cheat, steal, or smuggle just once. Inevitably, if they succeed the first time, they try again and again.

Since these repeat violations can be spotted and sanctioned by legitimate companies, criminals have to gravitate to the environments where the controls are weakest.

But the approach a smuggler takes to smuggling a WMD into the United States is likely to be different. First, terrorists may have to spend years acquiring 1-2 weapons. Once they have them, they are likely to be more than content to be successful on their first and only attempt. Since they know legitimate companies are viewed with much less scrutiny by U.S. authorities, it is these companies that present the best opportunity to get into the United State undetected if they can identify and exploit a vulnerability. Since no company has a fail-safe security system, they can be confident that they can locate and successfully compromise an existing safeguard at least once. It may be as simple as offering a large bribe to a truck driver to take an extended lunch break so that operatives can gain access to his load. A driver who repeatedly takes long lunch breaks might be noticed by a company with tight security controls. But only under extraordinary circumstances would a company have a system in place to detect such an infraction in real time the first time it takes place, particularly if the incident happens in overseas location between the factory where the container is stuffed and the loading port where it is being shipped to the United States. The only hope CBP has of detecting such a scenario is to have routine access to reliable intelligence about the identities and activities of terrorists. But this is a very weak reed to rely upon given the current difficulties the U.S. intelligence community is facing in adapting to the counter-terrorism mission.

The second reason for a terrorist organization to explicitly target a C-TPAT participant is that a successful penetration will have the derivative advantage of eroding public trust in the U.S. government's risk-management model. If a terrorist group can succeed at carrying out a WMD attack with what CBP has declared to be a "low-risk" container, all containers thereafter will be viewed as "high-risk." This will inevitably generate irresistible political pressure to subject all containers to a comprehensive inspection. The resultant widespread economic and societal disruption and billions of dollars of costs which would arise from a post-attack "100 percent" inspection regime would have real military value for our enemies.

3. The lack of specific standards under C-TPAT that are uniformly enforced is undermining the incentive for legitimate companies to invest in upgraded supply chain security measures. Security is not free. A C-TPAT participant incurs costs when it invests in measures to bolster its security protocols. Given the sheer numbers of companies participating in the program and the well-advertised lack of CBP's capacity to validate compliance, companies that are sincerely committed to improving their security have to worry about the likelihood that it has competitors who end up being free riders. In other words, they have to be mindful of potentially putting themselves at a competitive disadvantage by investing in security while others are doing little to nothing but receiving the same benefits from CBP. Absent a sense that there is a level playing field, executives become understandably reluctant to do more than the bare minimum to comply.

4. To the extent that resource constraints prevent CBP from extending CSI to less developed countries, we may end up indirectly creating a barrier to trade with those

nations. This then has the unintended consequence of eroding the development prospects for those countries, thereby creating the very conditions that fuel the terrorist threat.

5. There are conflicts between the operation of CSI and C-TPAT and the International Ship and Port Facility Security Code (ISPS) that came into effect on 1 July 2004. ISPS establishes minimum international security requirements for all ocean carriers and marine terminals, but does not address the cargo security issue. C-TPAT places requirements which are redundant or exceed the ISPS mandates on ocean carriers and marine terminals but participation is voluntary. CSI places some poorly defined requirements on the ports who are participating, but it is not a universal program. Consequently, should there be intelligence of a pending attack or an actual attack that results in maritime authorities elevating the ISPS three-tiered alert level, CBP's promised benefit of greater facilitation will be compromised. This is because a ship will almost always be carrying containers that are mixture of C-TPAT and non-C-TPAT participants and which originate from both CSI and non-CSI ports. Therefore, as a practical matter, under the rules governing the ISPS code, the ship and the receiving terminal will be subjected to the same heightened security requirements and the associated delays regardless of whether or not the cargo is from a C-TPAT company and a CSI port.

The shortcomings I have outlined above are very serious, but they all can be addressed at a reasonable cost, making it possible to advance the very positive objectives that spawned CSI and C-TPAT in the first place.

1. The way to advance the credibility of C-TPAT is for DHS to authorize third parties to conduct the validation audits of the proposed security protocols. DHS can require that these companies post a bond as a guarantor against substandard performance. These third parties will need to be given some liability protection by the federal government should their good-faith efforts fail. DHS must also have the means to "audit the auditors" to maintain high standards.

There are models for this. In the maritime area, the Coast Guard has long authorized "professional classification societies" to conduct inspections to determine if a ship is compliant with international shipping safety standards. These third party organizations are able to maintain the requisite technical expertise at a higher level than is possible within the federal government. They are also able to operate in overseas jurisdictions where U.S. officials may not be welcome. To keep the system honest, the Coast Guard periodically inspects vessels entering U.S. waters. Should it find that the vessel is in violation of the international standards, it will not only hold up that ship until corrective actions are taken, but it will target for inspection all other vessels who have been certified by the same classification society.

2. To minimize the risk that containers from C-TPAT participants will be targeted by terrorist organizations between the factory and the loading port, the U.S. government needs to work with the European Union and its other allies in advancing a standard for tracking a container and monitoring its integrity. The Radio Frequency Identification (RFID) technologies now being used by the Department of Defense for the global

movement of military goods can provide the foundation for putting in place such a regime.

3. The U.S. government should endorse a pilot project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong in which every container arriving in the two of the busiest marine terminals in the world are, at average speeds of 15 kph, passing through gamma ray machine, a radiation portal, and optical character recognition cameras which record the container number. These images and radiation profiles are then being stored in a database allowing the virtual inspection of any and all containers entering the terminal. The cost of deploying and maintaining this system throughout the entire port it estimated to be $6.50 per container.

The port of Hong Kong has invested in this system for three reasons. Most importantly, they are hoping that this 100 percent scanning regime will deter a terrorist organization from placing a WMD in a container passing through their port. Second, should a container be targeted under the CSI agreement between CBP and Hong Kong Customs & Excise, the system will allow the box to be inspected without the importer having to pay for the "service" of having the container removed from the marine terminal, transported to a Customs & Excise inspection facility, and returned by which time it would almost certainly miss its scheduled voyage. Last, by maintaining a record of the contents of every container entering their terminal, the port is able to provide government authorities with a forensic tool that can support a follow-up investigation should a container still slip through with a WMD. Their incentive to do so is that if an incident can be quickly isolated to a single supply chain then there will be no need for a port-wide shut down. In other words, by scanning every container, they are well positioned to indemnify the port as the source of a potential security breech. As result, a terrorist would be deprived of the collateral consequence of mass disruption of the intermodal transportation system.

This low-cost system of inspection is being carried out with no adverse impact on the marine terminals operations and without any U.S. government funding. It could be put in place globally at a cost of $1.5 billion or roughly $10 per container. Along with the third party inspection of C-TPAT compliance, establishing standards that support the deployment of "smart" containers at an estimated cost of $50 per shipment, we can move from the current "trust, but don't verify" system to a "trust but verify" one. Can industry afford the cost of this regime? To put the figures into context, the average container moved by Target or Wal-Mart from Asia to the United States carries approximately $60,000 in merchandise. Even a total of $100 additional cost per container would raise the price of those goods by .06 percent. What consumers are getting in return for that investment is both the reduced risk of a WMD attack and the cascading economic consequences flowing from such an attack which could hold the potential of generating a global recession. In short, this is about the soundest investment that they could make towards buying an added measure of security in our post-9/11 world.

4. The U.S. Department of State should lead a federal effort to have international development organizations; e.g., the World Bank, regional banks, WTO, etc., provide the

less develop countries with the non-intrusive inspection equipment, training, and data management tools to examine cargo entering and leaving their jurisdictions.

5. CSI and C-TPAT should be linked to the ISPS code.

When Commissioner Bonner first announced what has become the Container Security Initiative in a speech at CSIS in January 2002 he said:

> *As with any new proposal, implementation of this initiative will not be easy. But the size and scope of the task pale in comparison with what is at stake. And that is nothing less than the integrity of our global trading system upon which the world economy depends.*

These words are as true today as they were just four months after 9/11. What is required as we move forward is a willingness to both critically evaluate where we are and to make mid-course adjustments that keep us steaming rapidly ahead. That is why the oversight work of this committee and this hearing today is so important.

The biggest barrier to progress right now is the reluctance by DHS to make several necessary mid-course changes:

CBP has been resistant to the idea of 3rd party inspectors for C-TPAT compliance even though: (a) they are hopelessly behind in processing applications, (b) they have only a few inspectors who currently have adequate experience and training in supply chain security, and (c) they lack the legal authority to carry out validation inspections overseas.

While CBP has been generally supportive of deploying electronic container seals, they have shown little interest in technologies that could monitor the location of containers as they move through the transportation system. They also have not yet communicated to the port of Hong Kong an indication of their interest or support for the cargo container inspection project now underway there.

My experience interacting with CBP on these initiatives over the past 3 ½ years is that their ambivalence about embracing new technologies that are deployed to confirm that low risk participants in the trade system are indeed low risk stems from four sources. First, they are reluctant to acknowledge that many of their pre-9/11 risk management assumptions may not be well-suited for the low-probability but high consequence threat posed by the WMD in a container. Second, they are reluctant to "deputize" to the private sector functions historically performed by customs agents. Third, beyond the requirement that ocean carriers provide them with cargo manifests, they have traditionally maintained nominal interactions with the transportation industry, focusing instead on importers and exporters and trade intermediaries. Last, they are queasy about being given more data than they are in a position to examine and analyze. This creates a collateral bureaucratic risk of being held accountable should a post-mortem investigation reveal that they had data in their possession, but failed to look closely at it.

But my experience has also been that CBP is populated with dedicated and hardworking professionals who take their jobs extremely seriously. They work with far fewer resources than they deserve and receive too little credit for the important job they perform each day. C-TPAT and CSI demonstrates their ability to be both innovative and adaptive in the face of a new threat. These programs deserve the support of the administration, the Congress, and the American people. But, much work remains to be done towards ensuring they are a match for the catastrophic terrorist threat we face in the 21st century.

Prepared Testimony by C. Stewart Verdery, Jr.
Principal, Mehlman Vogel Castagnetti, Inc.
Adjunct Fellow, Center for Strategic & International Studies

U.S. Senate Committee on Homeland Security and Governmental Affairs
Permanent Subcommittee on Investigations
"The Container Security Initiative and the Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?"

Washington, D.C.
May 26, 2005

INTRODUCTION

Chairman Collins, Chairman Coleman, Ranking Member Lieberman, and Ranking Member Levin, thank you for the opportunity to return to your committee to discuss critical issues related to supply chain security. I am currently a principal at the consulting firm Mehlman Vogel Castagnetti, Inc. I also serve as an Adjunct Fellow at the Center for Strategic & International Studies, although the views in this testimony are my own and do not represent CSIS which does not take policy positions.

As you know, following action by this Committee and confirmation by the Senate in 2003, I served as Assistant Secretary for Border and Transportation Security Policy and Planning until my resignation from the Department of Homeland Security in March of this year. In this capacity, I was responsible for policy development within the Border and Transportation Security Directorate, reporting to Under Secretary Asa Hutchinson and Secretary Tom Ridge. BTS was created to coordinate policy development and operational activities in the fields of immigration and visas, transportation security, law enforcement, and cargo security which were largely carried out in the field by BTS agencies – U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration.

Before discussing the specific topics which are the subject of this important hearing, I would be remiss if I did not thank this Committee for its extremely important efforts to support DHS during my tenure at the Department. Among other accomplishments in this regard were last year's intelligence reform bill enacted last year, which included significant sections on border security and transportation security in addition to the intelligence provisions; the partial realignment of oversight of DHS within the Senate; and the day-to-day oversight of our activities which helped focus our priorities and responsiveness to the American people.

As a last introductory point, to the extent that legitimate analysis finds fault with the cargo security measures implemented by DHS over the past two years, I accept a large measure of responsibility for those shortcomings. I am proud of the efforts the first leadership of the Department under Secretary Tom Ridge. I strongly believe our initiatives have reduced the vulnerability of our country to terrorist attacks, including

attacks related to international shipping, but I also recognize that the country is still at the front end of a lengthy effort to craft policies and develop operational capabilities before we might be able to declare victory in this fight.

BACKGROUND

Today's hearing addresses the effectiveness of two of the major programs deployed by DHS to secure our international supply chain and global trade. This steady march of cargo containers and other types of international trade is the vehicle that drives our economy and provides for our prosperity. Poorly devised security programs would be the equivalent of driving this well-oiled-vehicle with the parking brake on: the damage to our way of life could be as great as any plot contrived by Osama bin Laden and his sympathizers. However, the massive scale and complexity of the processes which brings goods and materials from around the world to our tables, shelves, plants, and offices also represents an enormous vulnerability for the importation of terrorists or terrorist weapons.

People often ask me if we are safe and my answer is usually that we are safer but we are not safe. Since September 11th, we have reengineered our economy, our law enforcement focus, our intelligence system, and international travel practices, and have produced tremendous results in the war on terrorism.

Under the leadership of Commissioner Robert Bonner, the former U.S. Customs Service and current U.S. Customs and Border Protection have designed and implemented a series of innovative programs to secure international trade. While we should always strive to improve these initiatives, no discussion of this issue would be complete without recognizing the tremendous achievements to date: dozens of foreign ports allowing our inspectors to "push the borders out"; extensive information being submitted for review on each shipment, thousands of companies stepping up to the plate with aggressive and thorough security programs; the stand-up of the National Targeting Center; agreement with the European Union to develop common technical standards and inspection regimes; and leadership in world standard setting bodies in building a global consensus for supply chain security.

Thus, I strongly disagree with any analysis that argues that we are somehow worse off with the Container Security Initiative, the Customs-Trade Partnership Against Terrorism, and related programs in place than we would be without them. Minor program flaws due to budget needs, operational or technology limitations, or necessary integration with other initiatives should not obscure the massive contribution to our security that these programs have delivered.

However, if you look at some of the other major homeland security issues facing the government, we have implemented soup-to-nuts overhauls in many areas: intelligence, visa policy, entry-exit systems, aviation security, and information-sharing. But we really have not done so with supply chain security. The programs that CBP, the Coast Guard, and other agencies have implemented are surely part of a plan, but they are not a strategy by themselves. We need to determine what our desired end-state is. What do we want

the cargo environment to look like over the next three to five years? How can we get from here to there? As Will Rogers said, "Even if you're on the right track, you'll get run over if you just sit there."

Before turning to the specific programs that are the subject of today's hearing, this overall framework into which they fit must be discussed. Throughout the past year, my former office developed a draft cargo security strategic framework distributed at the DHS Cargo Summit in Decembr of 2004. This effort was led by now-Acting Assistant Secretary Elaine Dezenski, working with CBP, TSA, the Coast Guard, and our Science and Technology Directorate, and directed by former Deputy Secretary Jim Loy and former Under Secretary Hutchinson. Following comments from a wide range of stakeholders and analysis by the Homeland Security Institute, a comprehensive national strategy for cargo security is now in final development as part of the Secretary's "Second Stage Review" of DHS organizational structures and policy priorities.

First and foremost in the strategy, we must adopt a zero tolerance policy towards the arrival of weapons of mass destruction at our borders, beginning with radiological and nuclear threats. CBP is already in the processes of deploying equipment to detect radiation at U.S. ports, but we must address a number of lingering questions: Can the reliability and sensitivity of these systems be improved? Can we minimize the amount of cargo that arrives at U.S. ports without having been screened for WMD? And most importantly, is our current balance of resources and programmatic priorities properly structured to achieve this objective? The recent announcement by the S&T Directorate seeking next generation detection devices is a positive step toward making sure we are seeking and deploying the best possible equipment in the area. The development of the proposed Domestic Nuclear Detection Office also represents an opportunity to steer resources and attention to this most urgent priority.

Second, while the admissibility decision will always be one of DHS's most powerful authorities, we must be able to make more informed decisions. This will require more information from segments of the supply chain we do not currently have visibility into.

The U.S. Coast Guard is working with its sister agencies in DHS and throughout the federal government to develop a system for Maritime Domain Awareness. Through this effort, the Coast Guard will deploy a capability to track vessels in our ports and coastal approaches, providing DHS with additional knowledge about ships that are carrying the cargo we are investing so much in to secure. Much of this work is being carried out under the rubric of Homeland Security Presidential Directive 13 issued by the President last December.

Third, DHS is also committed to improving our awareness of individual shipments through the application of secure stuffing procedures and in-transit intrusion detection. The best evidence that something is awry with an international shipment is physical evidence of tampering. DHS has no such awareness today. As a short-term solution, DHS will soon mandate the use of high security mechanical seals on all loaded, in-bound containers. Via Operation Safe Commerce and the Advanced Container Security Device

program, DHS plans to bring to market vastly improved capabilities over the next five years.

This growth will require effective tools for processing information. The rapid build-out of the Automated Commercial Environment (ACE) platform for targeting and selectivity across modes is a top priority for DHS. The Administration and Congress should support ACE as the single portal for trade data submitted to DHS and the root analytical capability for all cargo and trade related targeting. This approach will eliminate redundancies, promote consistency in the operational environment, and simplify interfaces with DHS. This tenant of the framework clearly exemplifies the dual mission of security and facilitation.

CSI AND C-TPAT

Turning to the specific programs reviewed by GAO, GAO's critiques of the programs appear to be accurate generally, an assessment that DHS and CBP appear to share. I normally found GAO's review of DHS initiatives to provide constructive analysis and view these reports in a similar fashion.

In terms of CSI, I completely agree with the GAO suggestion that CBP and DHS redouble efforts to ensure that sufficient personnel are assigned overseas to conduct targeting operations. Obtaining approvals, funding, and space to assign DHS personnel overseas has proved to be a difficult problem, not only in the CSI context, but also for the Visa Security Program authorized by the Homeland Security Act. However, to the extent that certain targeting operations can be conducted in the United States at the National Targeting Center, as opposed to overseas, personnel overseas should be encouraged to spend that extra time developing relationships with local law enforcement and customs officials to develop more leads than can make that targeting all the more valuable. Further, for CSI teams which include special agents from Immigration and Customs Enforcement, if freed up from conducting targeting operations, these agents should be able to provide valuable assistance to other DHS missions in the host country beyond cargo security. It is also important that CSI team members, to the greatest extent possible, be stationed for as long as a term as possible to minimize personnel rollover that hinders development of the personal relationships with host country customs and law enforcement officials that are the most likely mechanism for developing leads and targeting concepts.

In terms of C-TPAT, the effectiveness of CBP in attracting companies to apply has changed the overall dynamic of the program. In addressing a key priority of Under Secretary Hutchinson and myself, CBP has committed to hiring a significant number of new validators to ensure that promises made are being implemented. But as GAO points out, the total number of members who have been validated is still just a small fraction of the overall members, or even those whose paperwork has been certified to be in order. It clearly should be a priority for CBP to continue to increase the number of validators and to vastly increase the percentage of enrollees who have received a robust validation. Part of the solution may be to slow down recruitment of new C-TPAT members.

However, for the many thousands of companies, especially importers, who have enrolled and are awaiting validation, the question remains how their shipments should be handled. I understand that CBP has recently introduced a tiered system to provide some, but not full, benefits for such companies as their cargo is being evaluated by CBP's Automated Targeting System. This strikes me as a reasonable risk assessment to prioritize inspection activities on those about whose security practices we know very little, but to withhold full facilitation benefits pending validation.

It is worth noting that many of the critiques of C-TPAT in the GAO report have been highlighted in the Maritime Transportation Security subcommittee of the Commercial Operations Advisory Committee (COAC) which Under Secretary Hutchinson and I chaired at DHS. This subcommittee provided valuable feedback to DHS, BTS, and CBP as to proposed improvements in C-TPAT.

In addition, C-TPAT has undergone significant strengthening since the underlying work in this GAO report was concluded. In March of this year, following extensive vetting with the trade and within DHS and BTS, CBP announced new guidelines for existing and future C-TPAT members. New requirements for hardening of physical security requirements, internal security requirements, and business partner security requirements will represent, when implemented in phases, a major leap forward in the effectiveness of C-TPAT.

How to measure that effectiveness continues to present a major challenge for DHS. CBP has struggled with appropriate performance measures that would capture the value of C-TPAT to security and the benefit to enrolled partners. While the sheer numbers of participating companies and percentage of cargo that arrives under the framework of CSI and/or C-TPAT are useful statistics, they probably do not actually capture the deterrence value of the programs, nor the value they represent in detecting the needles in the cargo haystack. It is perhaps unremarkable that such performance measures have been elusive as the government has struggled to quantify the effectiveness of similar programs designed to fight crime or interdict drugs. As DHS improves its ability to conduct strategic planning, the department should continue to strive for such performance measures, with the understanding that no perfect analytical system is likely to emerge.

Lastly, I believe that DHS and the Congress should begin to review whether C-TPAT should be transformed into a more typical regulatory framework. As the guidelines become more and more a de facto industry standard and place more and more demands on the trade, converting C-TPAT into a series of regulations that apply to all relevant players in the supply chain might provide more transparency into our public policy making and build more public confidence in those policies. The process by which DHS and CBP have developed and imposed C-TPAT guidelines is an unusual one, especially when compared to the massive legal framework of statutes and regulations that undergird CBP's other mission to implement our nation's immigration laws.

POLICY-MAKING AT DHS

This committee which holds jurisdiction over the organizational structure of DHS should take careful note that neither of the GAO reports discussed today even mention the existence of the Border and Transportation Security Directorate or any other segment of DHS which has a role in crafting department-wide policy. I have little doubt that if follow-up reports are conducted within the next year, DHS will have established a robust policy and planning office that will be the heart of long term strategic thinking about issues like supply chain security. The current structure of DHS has only a small and non-publicized policy arm reporting to the Secretary, although it was staffed by many excellent public servants. My former policy office situated in BTS has more staff, visibility and official responsibilities but lacked authority to force coordination between BTS agencies and other parts of the department such as the Coast Guard and the Science and Technology Directorate. And very little policy development has been incorporated into long-term budgeting or strategic planning.

The obvious solution to this shortcoming is a robust policy and planning office operating under expansive authority of the Secretary to resolve disputes between parts of the department, to identify departmental budget and policy priorities, and to integrate interaction with foreign governments and international organizations into policy development. Many commentators have associated this concept with the "DHS 2.0" paper authored by the Heritage Foundation and CSIS in 2004, but for those of us who labored under difficult resource and structural limitations after the creation of DHS, this office was a "no-brainer" from the start. I believe I speak for the entire former leadership team – including Secretary Ridge and Deputy Secretary Loy – in this regard and am extremely confident that this new office will emerge soon from Secretary Chertoff's "Second Stage Review" underway to develop improved structures and clear priorities for DHS.

CONCLUSION

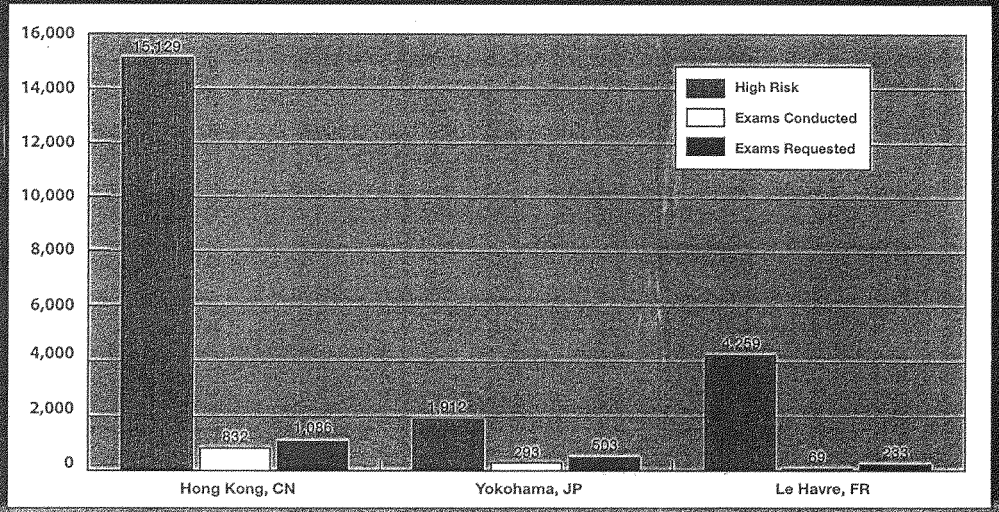
The title of today's hearing attempts to portray the work-to-date by DHS to secure supply chain security as a choice between complete success and failure. In reality, that work will always be a work in progress. Working under a strategic plan, each new programmatic decision, deployment of each piece of advanced technology, each commitment by a private sector entity, and each hard day of work by our nation's front-line inspectors, investigators, and analysts is a brick in the wall of security that is being constructed.

I congratulate the Committee and Subcommittee for its continued cooperation with and oversight of DHS and its component agencies. I thank you for the opportunity to appear before you today and look forward to your questions.

Permanent Subcommittee on Investigations
EXHIBIT #1

High-Risk Shipments and Exams Conducted at Selected CSI Ports 2004

CSI Ports: Hong Kong, Yokohama, and Le Havre



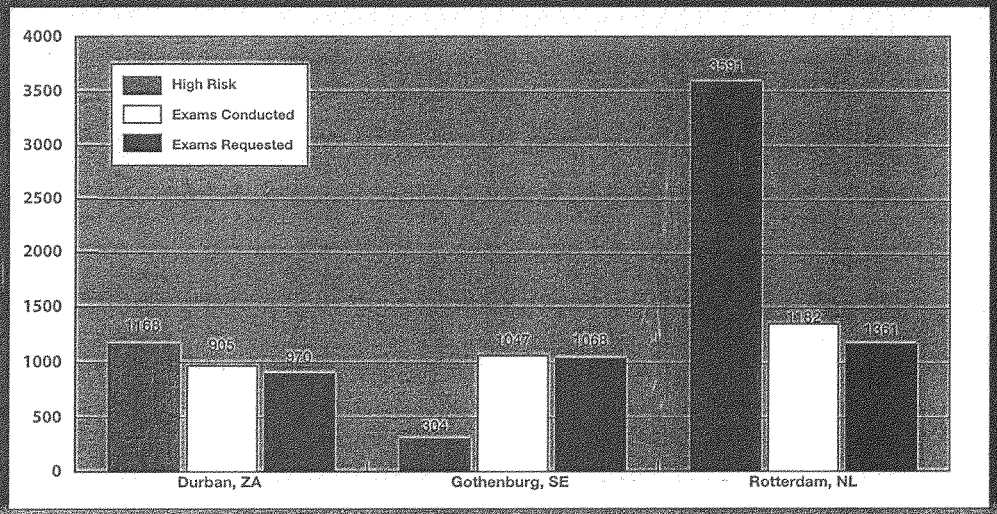
CSI Port	Total Volume	High Risk	% High Risk	Exams Requested	Exams Conducted	% of Exams Requested that were Actually Conducted	% of High Risk Shipments that were Examined	% Total Volume Examined
Hong Kong, CN	1,848,179	15,129	0.82%	1,086	832	76.61%	5.50%	0.06%
Yokohama, JP	90,243	1,912	2.12%	503	293	58.25%	15.32%	0.56%
Le Havre, FR	123,424	4,259	3.45%	233	69	29.61%	1.62%	0.19%

Permanent Subcommittee on Investigations

EXHIBIT #2

High-Risk Shipments and Exams Conducted at Selected CSI Ports 2004

CSI Ports: Durban, Gothenburg, and Rotterdam



CSI Port	Total Volume	High Risk	% High Risk	Exams Requested	Exams Conducted	% of Exams Requested that were Actually Conducted	% of High Risk Shipments that were Examined	% Total Volume Examined
Durban, Za	29,649	1168	3.94%	970	905	93.30%	77.48%	3.05%
Gothenburg, SE	10,484	304	2.90%	1068	1047	98.03%	344.07%	9.99%
Rotterdam, NL	245,104	3591	1.47%	1361	1182	86.85%	32.91%	.48%

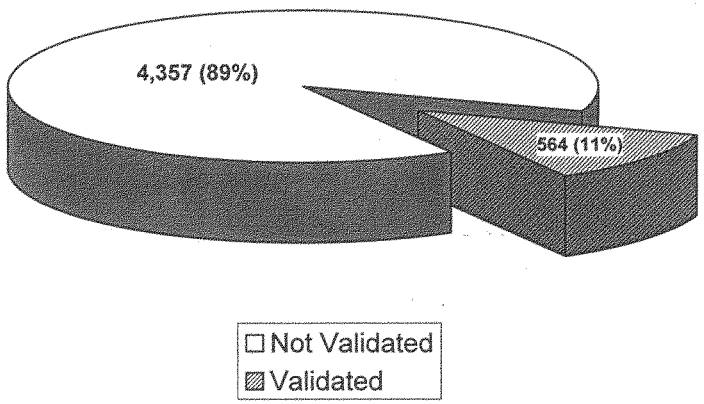
5145044 CSI Ports 1

5/25/05 3:27:03 PM

Status of Validating C-TPAT Members as of April 15, 2005

Total Applicants: 9,097

Certified Members
Total: 4,921
(52% of Total Applicants)



Permanent Subcommittee on Investigations
EXHIBIT #3

C-TPAT Membership Process

Application

Company submits information on a signed agreement to voluntarily participate.

Security Profile

Company completes a security profile and sends it to CBP within 60 days of submitting agreement.

Certification

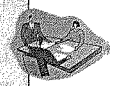
CBP reviews the supply chain security profile within 60 days of receipt. If the review is favorable, CBP sends the company a signed copy of the C-TPAT agreement. The member is then considered certified and benefits begin. For importers, however, benefits are not to be granted until successful completion of CBP's vetting process.

Vetting

For certified C-TPAT importers only, CBP conducts a separate vetting process to determine, through a compliance review and the violation history of the importer, if there is questionable information that might preclude approval of benefits. If the importer clears vetting, benefits are to begin within a few weeks. If not, benefits are not granted until successful completion of the validation process.

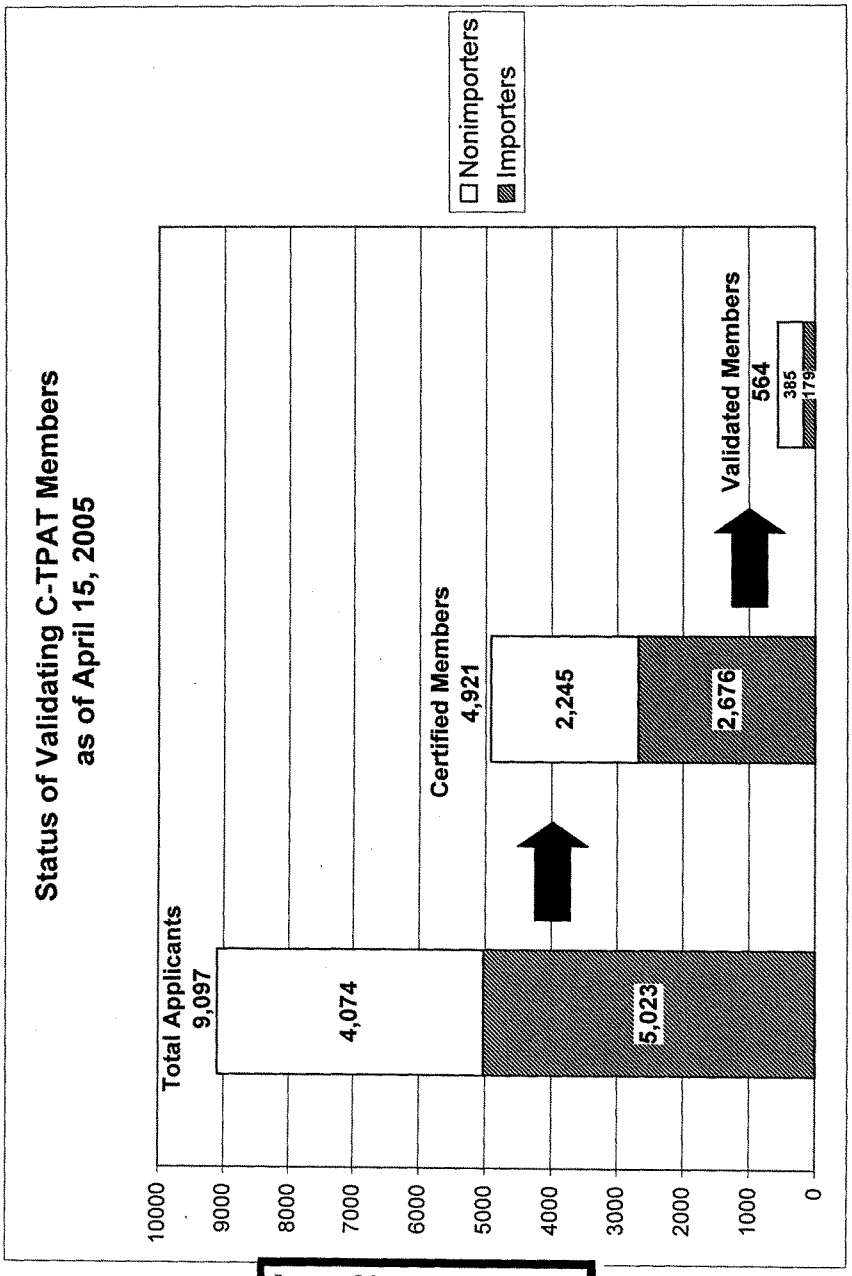
Validation

CBP conducts a validation of C-TPAT members to ensure they have implemented the security measures claimed in their supply chain security profiles. The validations are conducted jointly by CBP and a company representative. CBP provides the member with 30 days written notice before the validation commences. Validation results are documented in a final report and provided to the company.

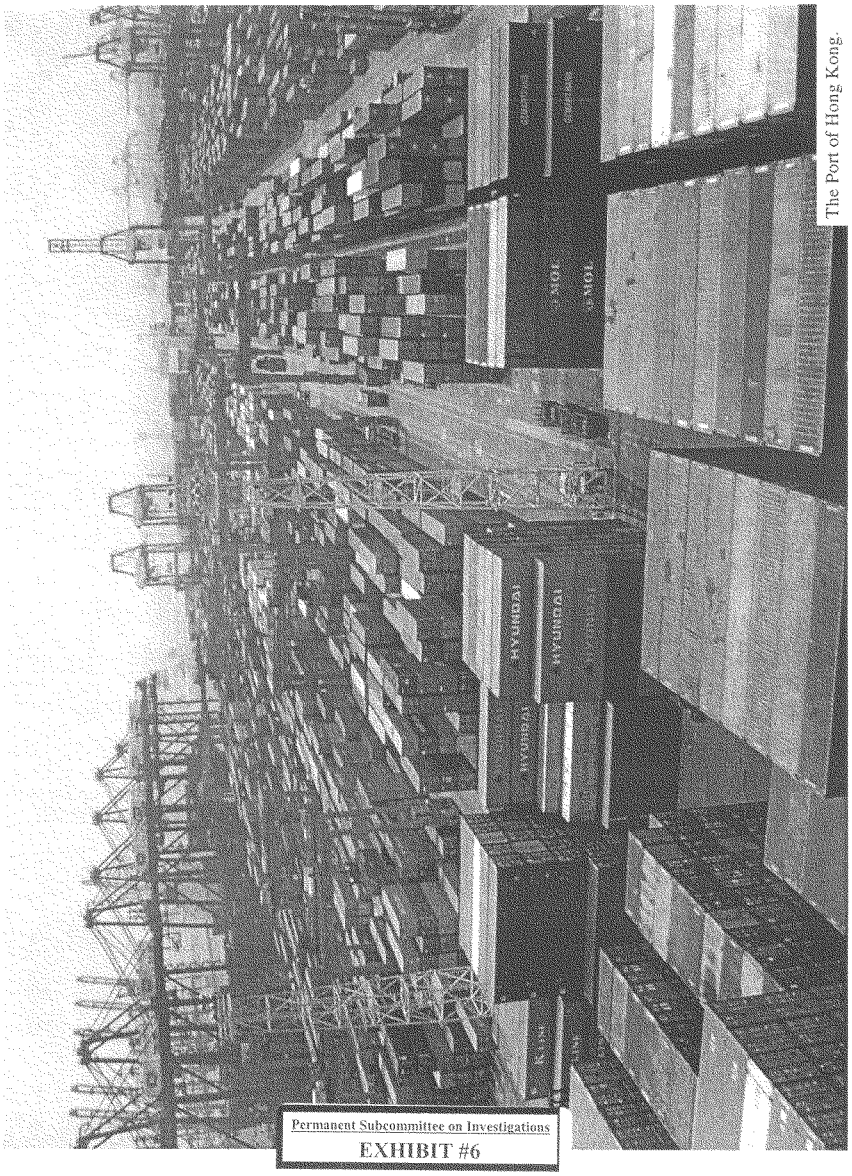


Permanent Subcommittee on Investigations

EXHIBIT #4



Permanent Subcommittee on Investigations
EXHIBIT #5



The Port of Hong Kong.

Permanent Subcommittee on Investigations
EXHIBIT #7

Heimann Mobile x-ray at the
Port of Felixstowe, England

United States Government Accountability Office

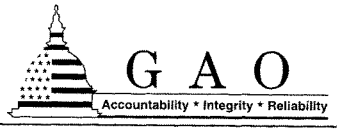
GAO

Report to Congressional Requesters

March 2005

CARGO SECURITY

Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security



GAO-05-404

Permanent Subcommittee on Investigations
EXHIBIT #8

Contents

Letter		1
	Results in Brief	3
	Background	6
	C-TPAT Benefits Reduce Scrutiny of Shipments	12
	CBP Grants Benefits before Verification of Security Procedures	13
	Weaknesses in Process for Verifying Security Procedures	14
	Incomplete Progress in Addressing Management Weaknesses	18
	Conclusions	21
	Recommendations for Executive Action	22
	Agency Comments and Our Evaluation	22
Appendix I	**Objectives, Scope, and Methodology**	27
	Objectives	27
	Scope and Methodology	27
	Data Reliability	27
Appendix II	**Comments from the Department of Homeland Security**	29
Appendix III	**GAO Contacts and Staff Acknowledgments**	34
	GAO Contacts	34
	Staff Acknowledgments	34
Related GAO Products		35
Tables		
	Table 1: Roles of Trade Community Members in the Supply Chain	8
	Table 2: Benefits for C-TPAT Members	13
Figures		
	Figure 1: CBP's Review Process for C-TPAT Membership	11
	Figure 2: Status of Validating C-TPAT Members, as of November 2, 2004	16

Abbreviations

ATS	Automated Targeting System
CBP	Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
FAST	Free and Secure Trade

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

United States Government Accountability Office
Washington, DC 20548

March 11, 2005

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

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

The Honorable John D. Dingell
Ranking Minority Member
Energy and Commerce Committee
House of Representatives

This report is a publicly available version of our report on the Customs-Trade Partnership Against Terrorism (C-TPAT). The Department of Homeland Security (DHS) designated our original report as Limited Official Use because of the sensitive and specific nature of the information it contained.

U.S. Customs and Border Protection (CBP), the DHS bureau responsible for protecting the nation's borders at and between the official ports of entry, has the dual goals of preventing terrorists and terrorist weapons from entering the United States and also facilitating the flow of legitimate trade and travel. Approximately 90 percent of the world's cargo moves by container. Addressing the threat posed by the movement of containerized cargo across U.S. borders has traditionally posed many challenges for CBP, in particular balancing the bureau's border protection functions and trade enforcement mission with its goal of facilitating the flow of cargo and persons into the United States. CBP has said that the large volume of imports and its limited resources make it impossible to physically inspect all oceangoing containers without disrupting the flow of commerce, and it is unrealistic to expect that all containers warrant such inspection.

To address its responsibility to improve cargo security while facilitating commerce, CBP employs multiple strategies. Among these strategies, CBP has in place an initiative known as C-TPAT, which aims to secure the flow of goods bound for the United States by developing a strong, voluntary antiterrorism partnership with the trade community. C-TPAT members commit to improving the security of their supply chain (flow of goods from manufacturer to retailer) and develop written security profiles that outline the security measures in place for the company's supply chain. In exchange for this commitment, CBP offers C-TPAT members benefits for participating that may reduce the level of scrutiny given to their shipments, potentially resulting in a reduced number of inspections of their cargo at U.S. borders.

The program is promising, but previous work has raised concerns about its management and its ability to achieve its ultimate goal of improved cargo security. Specifically, in our July 2003 report on this program, we recommended that the Secretary of Homeland Security work with the CBP Commissioner to develop (1) a strategic plan that clearly lays out the program's goals, objectives, and detailed implementation strategies; (2) performance measures that include outcome-oriented indicators; and (3) a human capital plan that clearly describes how C-TPAT will recruit, train, and retain new staff to meet the program's growing demands as it implements new program elements.[1]

Given our past concerns about the program's effectiveness and in light of the program's rapid expansion, we examined selected aspects of the program's operation and management. This report addresses the following issues:

1. What benefits does CBP provide to C-TPAT members?
2. Before providing benefits, what approach does CBP take to determine C-TPAT members' eligibility for them?
3. After providing benefits, how does CBP verify that members have implemented their security measures?
4. To what extent has CBP developed strategies and related management tools for achieving the program's goals?

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

To address all four objectives, we discussed program operations with CBP officials in Washington, D.C., with program responsibilities for C-TPAT and reviewed available data and documentation for the program. To ascertain the manner in which CBP validates security procedures for participating companies, we asked CBP to provide us with examples of participant files, including files of participants with responsibilities along various parts of the supply chain. While the files we reviewed were not a representative sample of files, we noted that in many cases these files were incomplete. We also reviewed CBP's database for tracking participant status in the program. Initial reliability testing of this database and interviews of staff with responsibility for the program led us to conclude that data used to track participant status had some serious reliability weaknesses. However, we found the data sufficiently reliable for limited use in describing the program's status. While we were able to review CBP's processes, because of the poor condition of member files we were unable to verify the extent that the bureau followed the processes in individual cases for individual members. We also examined the status of the agency's efforts to implement our prior recommendations for the program.

We conducted our work from February through December 2004 in accordance with generally accepted government auditing standards. More details about the scope and methodology of our work are presented in appendix I.

Results in Brief

In return for committing to making improvements to the security of their shipments by joining the program, C-TPAT members receive a range of benefits that reduce the level of scrutiny CBP provides to their shipments bound for the United States. These benefits may change the risk characterization of their shipments, thereby reducing the probability of extensive documentary and physical inspection. Other benefits include access to FAST lanes on the Canadian and Mexican borders, expedited cargo processing at FAST lanes, and an emphasis on self-policing and self-monitoring of security activities.[2] In addition, CBP grants benefits to C-TPAT members that do not directly affect the level of scrutiny given to their shipments. These additional benefits include a single point of contact within CBP to serve as a liaison with the member on issues related to the

[2]The Free and Secure Trade (FAST) program is a CBP program that allows Canadian and Mexican companies expedited processing of their commercial shipments at the border.

program, access to the identities of other companies that have become C-TPAT members, and eligibility to attend CBP-sponsored antiterrorism training seminars.

Before providing benefits, CBP uses a two-pronged approach to assess C-TPAT members. First, CBP has a certification process to review the self-reported information contained in applicants' membership agreements and security profiles. Second, CBP has in place a vetting process to try to assess the compliance with customs laws and regulations and violation history of and intelligence data on importers before granting them benefits. At the program's inception, CBP began granting benefits to C-TPAT applicants immediately upon receipt of their agreement to voluntarily participate in the program without any review of the security profiles submitted by potential member companies. In February 2004, CBP changed its policy to grant benefits to C-TPAT members only after CBP's review and certification of their security profiles and successful completion of the vetting process. CBP believes that this two-pronged approach provides adequate assurance before granting benefits. However, this approach grants benefits to members before they undergo the validation process.

After providing benefits, CBP has a validation process to verify that C-TPAT members' security measures have been implemented and that program benefits should continue. However, we found several weaknesses in the validation process that compromise CBP's ability to provide an actual verification that supply chain security measures in C-TPAT members' security profiles are accurate and are being followed. First, the validation process is not rigorous enough to achieve its stated purpose, which is to ensure that the security procedures outlined in members' security profiles are reliable, accurate, and effective. For example, CBP officials told us that validations are not considered independent audits, and the objectives, scope, and methodology of validations are jointly agreed upon with the member company. CBP officials, as well as our review of case files, indicated that the validations only examine a few of the security measures outlined in members' security profiles. Related to this, CBP has no written guidelines for its supply chain specialists to indicate what scope of effort is adequate for the validation to ensure that the member's measures are reliable, accurate, and effective. In addition, CBP has not determined the extent to which validations are needed. While the original stated goal of the program was to validate all members within 3 years, CBP decided that it could not do so because of the rapid growth in membership. In 3 years of C-TPAT operation, CBP has validated about 10 percent of its certified members. While CBP has given up on its original

goal to validate all members, it has not come up with an alternative goal for the number or percentage of members that should be validated. For validations that CBP does conduct, it prioritizes members for validation based on a variety of factors such as strategic threat, import volume, and past compliance violations.

While CBP has recently completed a strategic plan, we found weaknesses in some of the tools it uses to manage the program that could hinder the bureau in achieving the program's dual goals of securing the flow of goods bound for the United States and facilitating the flow of trade. CBP's new strategic plan appears to provide the bureau with a general framework on which to base key decisions, including key strategic planning elements such as strategic goals, objectives, and strategies. However, CBP still lacks a human capital plan, a fact that has impaired its ability to manage its resources. CBP officials told us they are in the process of developing an implementation plan that will address human capital planning elements such as analyzing (1) current workload, (2) the projected annual growth rate of the program, (3) the time it takes to complete the average validation, and (4) the number of validations supply chain specialists can complete annually. Furthermore, CBP still has not developed a comprehensive set of performance measures and indicators, including outcome-based measures, to monitor the status of program goals. CBP officials told us they have developed some initial measures to capture the program's impact. Finally, the C-TPAT program lacks an effective records management system. CBP's record keeping for the program is incomplete, as key decisions are not always documented and programmatic information is not updated regularly or accurately. For example, member files we reviewed contained no documentation of communications between CBP and members regarding how the scope of a validation was determined, and their database tracking member status contained errors.

We are making recommendations to the Secretary of the Department of Homeland Security to direct the U. S. Commissioner of Customs and Border Protection to improve the program's ability to meet its goals by providing appropriate guidance to specialists conducting validations, determining the extent to which members should be validated in lieu of the original goal to validate all members within 3 years of certification, and implementing performance measures, a human capital plan, and a records management system for the program. We provided a draft of this report to the Secretary of DHS for comment. In its response, from the Commissioner of U.S. Customs and Border Protection, CBP generally agreed with our recommendations and cited corrective actions they either have taken or planned to take.

Notwithstanding its general agreement with our recommendations, CBP noted that C-TPAT is a voluntary partnership to improve the security of the United States and not a program to confirm importer compliance with a regulatory requirement. As such, CBP said our report places too much emphasis on the validation process without adequately reflecting other aspects of the program. As a whole, CBP said that as part of its multilayered approach, C-TPAT identifies companies that take security seriously, appropriately lowers the risk level of their cargo, and thus focuses CBP resources on other companies' high-risk cargo, all consistent with a risk management approach. We believe that having a multilayered approach to cargo inspection can be effective, provided that each layer is adequately utilized. Given that C-TPAT members enjoy benefits that could greatly reduce the likelihood of an inspection of their cargo, not having full assurance of a reliable, accurate, and effective validation process potentially weakens the overall effectiveness of the other control mechanisms in meeting CBP's fundamental responsibility to ensure security of all cargo entering the United States. We fully address CBP's comments in the body of the report.

Background

CBP maintains two overarching goals: (1) increasing security and (2) facilitating legitimate trade and travel. Disruptions to the supply chain could have immediate and significant economic impacts.[3] For example, in terms of containers, CBP data indicates that in 2003 about 90 percent of the world's cargo moved by container.[4] In the United States, almost half of all incoming trade (by value) arrived by containers on board ships. Almost 7 million cargo containers arrive and are offloaded at U.S. seaports each year. Additionally, containers arrive via truck and rail. Therefore, it is vital for CBP to try to strike a balance between its antiterrorism efforts and facilitating the flow of legitimate international trade and travel.

Vulnerability of the Supply Chain

The terrorist events of September 11, 2001, raised concerns about company supply chains, particularly oceangoing cargo containers, potentially being used to move weapons of mass destruction to the United States. An extensive body of work on this subject by the Federal Bureau of

[3]A supply chain consists of all stages involved in fulfilling a customer request, including the manufacturer, suppliers, transporters, warehouses, and retailers.

[4]A container is a van, open-top trailer, or other similar trailer body on or into which cargo is loaded and transported.

Investigation and academic, think tank, and business organizations concluded that while the likelihood of such use of containers is considered low, the movement of oceangoing containerized cargo is vulnerable to some form of terrorist action. Such action, including attempts to smuggle either fully assembled weapons of mass destruction or their individual components, could lead to widespread death and damage.

The supply chain is particularly vulnerable to potential terrorists because of the number of individual companies handling and moving cargo through it. To move a container from production facilities overseas to distribution points in the United States, an importer has multiple options regarding the logistical process, such as routes and the selection of freight carriers. For example, some importers might own and operate key aspects of the overseas supply chain process, such as warehousing and trucking operations. Alternatively, importers might contract with logistical service providers, including freight consolidators and nonvessel-operating common carriers. In addition, importers must choose among various modes of transportation to use, such as rail, truck, or barge, to move containers from the manufacturer's warehouse to the port of lading. As shown in table 1, there are many players in the trade community, each with a role in the supply chain.

Table 1: Roles of Trade Community Members in the Supply Chain

Trade community member	Role in the supply chain
Air/rail/sea carriers	Carriers transport cargo via air, rail, or sea.
Border highway carriers	Highway carriers transport cargo for scheduled and unscheduled operations via road across the Canadian and Mexican borders.
Importers	Importers, in the course of trade, bring articles of trade from a foreign source into a domestic market.
Licensed customs brokers	Brokers clear goods through customs. The responsibilities of a broker include preparing the entry form and filing it, advising the importer on duties to be paid, and arranging for delivery to the importer.
Freight consolidators/ocean transportation intermediaries and nonvessel-operating common carriers	A freight consolidator is a firm that accepts partial container shipments from individual shippers and combines the shipments into a single container for delivery to the carrier. A transportation intermediary facilitates transactions by bringing buyers and sellers together. A nonvessel-operating common carrier is a company that buys shipping space, through a special arrangement with an ocean carrier, and resells the space to individual shippers.
Port authorities/terminal operators	A port authority is an entity of state or local government that owns, operates, or otherwise provides 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, overseeing the loading and unloading of railroad cars, and so forth.

Source: GAO.

According to research initiated by the U.S. Department of Transportation's Volpe National Transportation Systems Center, importers who own and operate the entire supply chain route from start to finish suffer fewer security breaches than others because they have greater control over their supply chains.[5] However, relatively few importers own and operate all key aspects of the cargo container transportation process, relying instead on second parties to move containerized cargo and prepare various transportation documents.

[5]Department of Transportation Volpe National Transportation Systems Center, *Intermodal Cargo Transportation: Industry Best Security Practices* (Cambridge, Mass.: June 2002).

CBP's Layered Enforcement Strategy

CBP has implemented a layered enforcement strategy to prevent terrorists and weapons of mass destruction from entering the United States through the supply chain.[6] A key element of this strategy is CBP's targeting and inspection of cargo that arrives at U.S. ports. For all arriving cargo containers, CBP uses a targeting strategy that employs its computerized targeting model, the Automated Targeting System (ATS). CBP uses ATS to review container documentation and help select, or target, shipments for additional documentary review or physical inspection. ATS is operated by CBP's National Targeting Center and is characterized by CBP as an expert system that uses hundreds of targeting rules to check available data for every arriving container, assigning a risk characterization to each container. The risk characterization helps to determine the type and level of scrutiny a container will receive. For example, CBP could review the container's bill of lading, examine the container with nonintrusive inspection equipment (that is, X-ray), or physically open the container. The extent of review varies, since according to CBP, the large volume of imports and CBP's limited resources make it impossible to physically inspect all containers without disrupting the flow of commerce.

Initiated in November 2001, C-TPAT is another element of CBP's layered enforcement strategy. C-TPAT is a voluntary program designed to improve the security of the international supply chain while maintaining an efficient flow of goods. Under C-TPAT, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security. In return for committing to making improvements to the security of their shipments by joining the program, C-TPAT members may receive benefits that result in reduced scrutiny of their shipments (e.g., reduced number of inspections or shorter border wait times for their shipments). C-TPAT membership is open to U.S.-based companies in the trade community, including (1) air/rail/sea carriers, (2) border highway carriers, (3) importers, (4) licensed customs brokers, (5) air freight consolidators and ocean transportation intermediaries and nonvessel-operating common carriers, and (6) port authorities or terminal operators.[7] According to CBP officials, program membership has grown

[6]The layered enforcement strategy encompasses CBP programs including C-TPAT (addressed in this report), as well as the Container Security Initiative (CSI). CSI is an initiative whereby CBP places staff at designated foreign seaports to work with foreign counterparts to identify and inspect high-risk containers for weapons of mass destruction before they are shipped to the United States. We are currently reviewing the CSI program and a report is forthcoming.

[7]In addition, there are hundreds of foreign-based air, rail, sea, and truck carriers certified in C-TPAT.

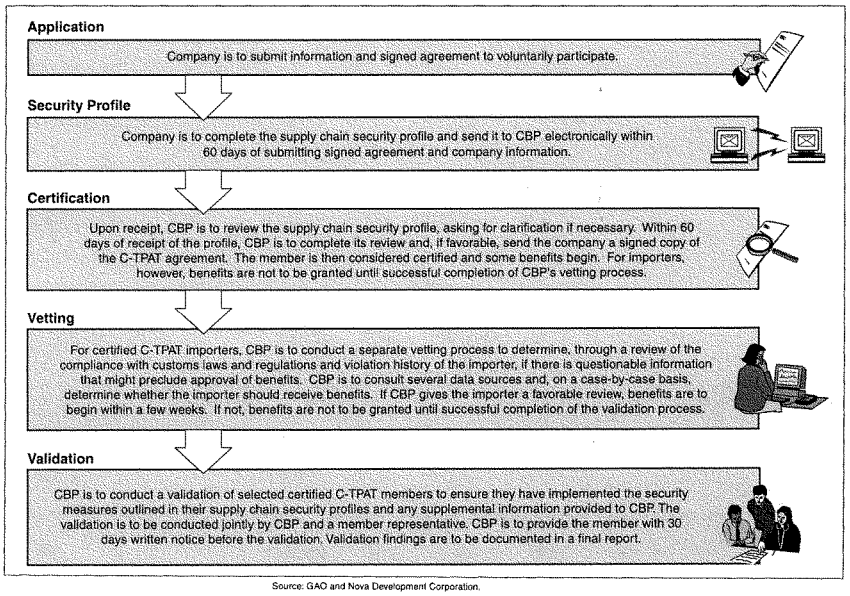
rapidly, and continued growth is expected, especially as member importers are requiring their suppliers to become C-TPAT members. For example, as of January 2003 approximately 1,700 companies had become C-TPAT members. By May 2003, the number had nearly doubled to 3,355. According to CBP officials, as of November 2004, the C-TPAT program had 7,312 members. For fiscal year 2004, the C-TPAT budget was about $18 million, with a requested budget for fiscal year 2005 of about $38 million for program expansion efforts. As of August 2004, CBP had hired 40 supply chain specialists, who are dedicated to serve as the principal advisers and primary points of contact for C-TPAT members.[8] The specialists are located in Washington, D.C., Miami, Florida, Los Angeles, California, and New York, New York.

CBP has a multistep review process for the C-TPAT program. As figure 1 shows, applicants first submit signed C-TPAT agreements affirming their desire to participate in the voluntary program. Applicants must also submit security profiles—executive summaries of their company's existing supply chain security procedures—that follow guidelines jointly developed by CBP and the trade community. These security profiles are to summarize the applicant's current security procedures in areas such as physical security, personnel security, and education and training awareness.[9] CBP established a certification process in which it reviews the applications and profiles by comparing their contents with the security guidelines jointly developed by CBP and the industry, looking for any weaknesses or gaps in the descriptions of security procedures. Once any issues are resolved to CBP's satisfaction, CBP signs the agreement and the company is considered to be a certified C-TPAT member, eligible for program benefits. Members that are not importers begin receiving benefits at this point, but members that are importers must undergo another layer of review, as described below. CBP encourages members to conduct self-assessments of their security profiles each year to determine any significant changes and to notify CBP. For example, members may be using new suppliers or new trucking companies and would need to update their security profiles to reflect these changes.

[8]For fiscal year 2004, CBP had authorization for 157 positions for supply chain specialists and support staff, but as of August 2004 had hired only 40 specialists. CBP officials noted that the bureau recognizes the need for additional permanent positions, and CBP plans to hire, train, and have in place an additional 30 to 50 supply chain specialists by the end of calendar year 2004.

[9]CBP established security guidelines to assist companies in completing their security profiles. Each set of security guidelines is tailored according to member type.

Figure 1: CBP's Review Process for C-TPAT Membership



Source: GAO and Nova Development Corporation.

For certified importers, CBP has an additional layer of review called the vetting process in which CBP reviews information about an importer's compliance with customs laws and regulations and violation history. CBP requires the vetting process for certified importers as a condition of granting them key program benefits. As part of the vetting process, CBP obtains trade compliance and intelligence information on certified importers from several data sources. If CBP gives the importer a favorable review, benefits are to begin within a few weeks. If not, benefits are not to be granted until successful completion of the validation process (see below).

The final step in the review process is validation. CBP's stated purpose for validations is to ensure that the security measures outlined in certified members' security profiles and periodic self-assessments are reliable, accurate, and effective. In the validation process, CBP staff meet with company representatives to verify the supply chain security measures contained in the company's security profile. The validation process is designed to include visits to the company's domestic and, potentially, foreign sites. The member and CBP jointly determine which elements of the member's supply chain measures will be validated, as well as which locations will be visited. Upon completion of the validation process, CBP prepares a final validation report it presents to the company that identifies any areas that need improvement and suggested corrective actions, as well as a determination if program benefits are still warranted for the member.

We have conducted previous reviews of the C-TPAT program and CBP's targeting and inspection strategy. In July 2003, we reported that CBP's management of C-TPAT had not evolved from a short-term focus to a long-term strategic approach.[10] We recommended that the Secretary of Homeland Security work with the CBP Commissioner to develop (1) a strategic plan that clearly lays out the program's goals, objectives, and detailed implementation strategies; (2) performance measures that include outcome-oriented indicators; and (3) a human capital plan that clearly describes how C-TPAT will recruit, train, and retain new staff to meet the program's growing demands as it implements new program elements. In March 2004, we testified that CBP's targeting system does not incorporate all key elements of a risk management framework and recognized modeling practices in assessing the risks posed by oceangoing cargo containers.[11]

C-TPAT Benefits Reduce Scrutiny of Shipments

CBP officials cite numerous benefits to C-TPAT members. As table 2 shows, these benefits may reduce the scrutiny of members' shipments. These benefits are emphasized to the trade community through direct marketing in presentations and via CBP's Web site. Although these benefits potentially reduce the likelihood of inspection of members'

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

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

shipments, CBP officials noted that all shipments entering the United States are subject to random inspections by CBP officials or inspections by other agencies.

Table 2: Benefits for C-TPAT Members

Benefit	Reduces amount of scrutiny provided for members?
A reduced number of inspections and reduced border wait times	Yes
Reduced selection rate for trade-related compliance examinations	Yes
Self-policing and self-monitoring of security activities	Yes
Access to the expedited cargo processing at designated FAST lanes (for certified highway carriers and certified importers along the Canadian and Mexican borders, as well as for certified Mexican manufacturers)	Yes
Eligible for the Importer Self-Assessment Program and has priority access to participate in other selected customs programs (for certified importers only)	Yes
A C-TPAT supply chain specialist to serve as the CBP liaison for validations	No
Access to the C-TPAT members list	No
Eligible to attend CBP-sponsored antiterrorism training seminars	No

Source: CBP's C-TPAT Strategic Plan, January 2005.

CBP Grants Benefits before Verification of Security Procedures

CBP has in place a two-pronged process to review members' qualifications for program benefits. First, CBP has a certification process to review the applications and security profiles submitted by applicants for any weaknesses or gaps in security procedures. CBP officials told us that during the certification process, it compares the members' security profiles against the C-TPAT security guidelines. Under the process, if there are any missing or unclear items, CBP is supposed to contact the member for clarification of those items. If the issues are resolved, CBP considers the member to be certified. However, if CBP determines that the security profiles contain weaknesses, CBP is not supposed to certify the member. According to CBP, approximately 20 percent of applications are not immediately certified because of initial shortcomings with the security profiles. However, CBP has stated that a company will not be rejected from participating in C-TPAT if there are problems with its security profile. Instead, CBP says it will work with companies to try to resolve and overcome any deficiencies with the profile itself.

Second, CBP has in place a vetting process to assess the compliance and violation history of importers before granting them benefits. If, in conducting the vetting process, CBP finds no prior negative compliance, violation, or intelligence information, it grants certified importers program benefits. According to CBP, to date most certified members who have been vetted have proven to have favorable or neutral importing histories. CBP officials told us that not many members have been denied benefits.

At the program's inception in November 2001, CBP began granting benefits to applicants upon receipt of their application for C-TPAT membership without any review of the applicants' paperwork. In February 2004, CBP changed its policy to retroactively delay granting the benefits until after CBP reviewed and certified applicants' security profiles and completed the vetting process. By providing incentives to members to implement certain security measures and performing various levels of checks on these measures, the C-TPAT program aims to encourage the reduction of vulnerability throughout the supply chain. CBP established a certification process in which it reviews the applications and profiles by comparing their contents with the security guidelines jointly developed by CBP and the industry, looking for any weaknesses or gaps in the descriptions of security procedures. The vetting process, which is required for importers eligible to receive benefits, augments the certification process by providing information about past compliance and violations, which CBP officials told us may suggest whether members' security practices have historically been effective at reducing vulnerability to exploitation. In addition, the vetting process may disclose threat concerns by pulling in information contained in intelligence databases. Ultimately, however, neither the certification nor vetting process provides an actual verification that the supply chain security measures contained in the C-TPAT member's security profile are accurate and are being followed before CBP grants the member benefits. A direct examination of selected members security procedures is conducted later as part of CBP's validation process, as discussed below.

Weaknesses in Process for Verifying Security Procedures

After providing benefits, CBP has a validation process to verify C-TPAT members' security measures have been implemented and that program benefits should continue. However, we found weaknesses in the validation process in that CBP has not taken a rigorous approach to conducting validations and has not determined the extent to which validations are needed. These weaknesses limit the bureau's ability to ensure that the program supports the prevention of terrorists and terrorist weapons from entering the United States.

Validation Process Lacks Rigor to Achieve Stated Purpose

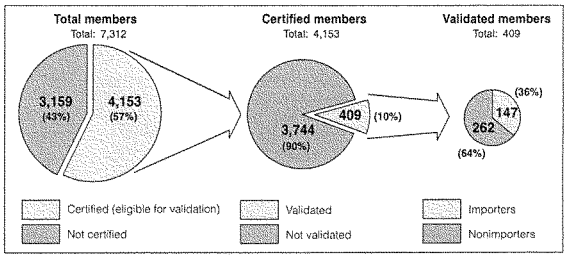
CBP's validation process is not rigorous enough to achieve its stated purpose, which is to ensure that the security procedures outlined in members' security profiles are reliable, accurate, and effective. While C-TPAT's stated purpose for validations is to ensure that the member's security measures are reliable, accurate, and effective, CBP officials told us that validations are not considered independent audits and the objectives, scope, and methodology of validations are jointly agreed upon with the member representatives. CBP has indicated that it does not intend for the validation process to be an exhaustive review of every security measure at each originating location; rather it selects specific facets of the members' security profiles to review for their reliability, accuracy, and effectiveness. For example, the guidance to ocean carriers for preparing a security profile directs the carriers to address, at a minimum, three broad areas (security program, personnel security, and service provider requirements), which contain several more specific security measures, such as facilities security and pre-employment screening. According to CBP officials, as well as our review of selected case files, validations only examine a few facets of members' security profiles. CBP supply chain specialists, who are responsible for conducting most of the validations, are supposed to individually determine which segments of a company's supply chain security will be suggested to the member for validation. To assist in this decision, supply chain specialists are supposed to compare a company's security profile, as well as any self-assessments or other company materials or information retrievable in national databases, against the C-TPAT security guidelines to determine which elements of the profile will be validated. Once the supply chain specialist determines the level and focus of the validation, the specialist is supposed to contact the member company with a potential agenda for the validation. The two parties then jointly reach agreement on which security elements will be reviewed and which locations will be visited.

CBP has no written guidelines for its supply chain specialist to indicate what scope of effort is adequate for the validation to ensure that the member's security measures are reliable, accurate, and effective, in part because it seeks to emphasize the partnership nature of the program. Importantly, CBP has no baseline standard for what minimally constitutes a validation. CBP discourages supply chain specialists from developing a set checklist of items to address during the validation, as CBP does not want to give the appearance of conducting an audit. In addition, as discussed later in the management section of this report, the validation reports we reviewed did not consistently document how the elements of members' security profiles were selected for validation.

CBP Has Not Determined the Extent to Which Validations Are Needed

CBP has not determined the extent to which it must conduct validations of members' security profiles to ensure that the operation of C-TPAT is consistent with its overall approach to managing risk. In 3 years of C-TPAT operation, CBP has validated about 10 percent of its certified members. CBP's original goal was to validate all certified members within 3 years of certification. However, CBP officials told us that because of rapid growth in program membership, it would not be possible to meet this goal. In February 2004, CBP indicated that approximately 5,700 companies had submitted signed agreements to participate in the program. As shown in figure 2, by November 2004, the number of members had grown to over 7,000, about 4,200 of which had been certified and thus eligible for validation. According to CBP, as of November 2004, CBP staff had completed validations of 409 companies, including 147 importers.

Figure 2: Status of Validating C-TPAT Members, as of November 2, 2004



Source: GAO analysis of CBP data.

CBP has made efforts to hire additional supply chain specialists to handle validations for the growing membership. As of August 2004, CBP had hired a total of 40 supply chain specialists to conduct validations, with 24 field office managers also available to conduct validations. CBP officials told us the bureau is currently conducting as many validations as its resources allow. However, CBP has not determined the number of supply chain specialists it needs or the extent to which validations are needed to provide reasonable assurance that it is employing a good risk management approach for the program.

CBP Considers Variety of Factors to Prioritize Validations

As noted above, CBP officials told us it would not be possible to meet the goal of validating every member within 3 years of certification. Instead, CBP is using what it calls a risk-based approach, which considers a variety of factors to prioritize which members should be validated as resources allow. CBP has an internal selection process it is supposed to apply to all certified members. Under this process CBP officials are supposed to prioritize members for validation based on established criteria but may also consider other factors.

CBP officials noted that other factors could affect the prioritization of members for validation. For example, recent seizures involving C-TPAT members can affect validation priorities. If a member is involved in a seizure, CBP officials noted that the member is supposed to lose program benefits and be given top priority for a validation. In addition, CBP officials told us that an importer that failed CBP's vetting process would also be given top priority for a validation. CBP officials have taken this approach because any importer that fails the vetting process is not supposed to receive program benefits until after successful completion of the validation process.

In August 2004, CBP began using a risk assessment tool developed for CBP's regulatory audits to assist in its prioritization of importers for validation. This tool ranks importers by risk according to factors such as value of imports, import volume, and method of transportation used by the importer for its goods.[12] CBP tailored the tool to consider only those factors it deemed relevant to C-TPAT. Applying the tool with this revised set of factors, CBP officials told us they produced a list that ranked each certified importer according to its risk. However, these ranked importers are then re-evaluated, along with members from other trade sectors, using CBP's internal selection process criteria. CBP officials told us that the human element provided by their internal selection process was important in prioritizing members for validation.

[12]CBP officials told us they are currently working to adapt the risk assessment tool so that it can be applied to C-TPAT members from additional trade sectors, such as brokers and carriers.

Incomplete Progress in Addressing Management Weaknesses

CBP continues to expand the C-TPAT program without addressing management weaknesses that could hinder the bureau from achieving the program's dual goals of securing the flow of goods bound for the United States and facilitating the flow of trade. In our July 2003 report, we recommended that the Secretary of Homeland Security work with the CBP Commissioner to develop (1) a strategic plan that clearly lays out the program's goals, objectives, and detailed implementation strategies; (2) a human capital plan that clearly describes how C-TPAT will recruit, train, and retain new staff to meet the program's growing demands as it implements new program elements; and (3) performance measures that include outcome-oriented indicators. While CBP agreed with our July 2003 recommendations, to date only one of them—the development of a strategic plan—has been implemented. According to CBP, the bureau is continuing to work on the July 2003 recommendations, which are in different stages of review.

CBP Has Finalized Its Strategic Plan

While a draft of this report was with DHS for comment, CBP issued a final strategic plan for C-TPAT on January 13, 2005. Our brief review of this plan indicates that it appears to clearly articulate the goals of the program, their relationship to broader CBP goals, and strategies for achieving them. For example, according to the plan there are five goals for the C-TPAT program:

1. ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria,
2. provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners,
3. internationalize the core principles of C-TPAT through cooperation and coordination with the international community,
4. support other CBP security and facilitation initiatives, and
5. improve administration of the C-TPAT program.

While we have not fully reviewed the strategic plan, it is a step in the right direction, and we encourage CBP to ensure that future plans include all of the key elements of a strategic plan as described in the Government Performance and Results Act of 1993. Specifically, the formal strategic plan should include a description of performance goals and how they are related to the general goals and objectives of the program, as well as a

description of program evaluations, which are useful for identifying key factors likely to affect program performance.

CBP Has Not Completed a Human Capital Plan

As a companion to developing a strategic plan for C-TPAT, CBP is developing an implementation plan to address the lower-level strategies for carrying out the program's goals. CBP told us it is still developing the implementation plan for the program but that it will include those elements required in a human capital plan. For example, CBP said it has developed new positions, training programs and materials, and a staffing plan. Further, CBP said the C-TPAT program will continue to refine all aspects of its human capital plan to include headquarters personnel, additional training requirements, budget, and future personnel profiles.

CBP Has Not Completed Development of Performance Measures

CBP has told us that it continues developing a comprehensive set of performance measures and indicators for C-TPAT. In support of the department's Future Years Homeland Security Program, CBP officials told us has identified 21 budget subactivities (programs, including C-TPAT) and has been tasked to develop two performance measures for each: (1) a main measure that would reflect program outcomes and (2) an efficiency measure that would reflect time or cost savings achieved through the program. CBP's Director, Strategic Planning and Audit Division, Office of Policy and Planning, noted that developing these measures for C-TPAT, as well as other programs in the bureau, has been difficult. The director noted that CBP lacks data necessary to exhibit whether a program has prevented or deterred terrorist activity. For example, as noted in the C-TPAT strategic plan, it is difficult to measure program effectiveness in terms of deterrence because generally the direct impact on unlawful activity is unknown. The plan also notes that while traditional workload measures are a valuable indicator, they do not necessarily reflect the success or failure of the bureau's efforts. CBP is working to collect more substantive information—related to C-TPAT activities (i.e., current workflow process)—to develop its performance measures. In commenting on a draft of this report, CBP indicated it has developed initial measures for the program but will continue to develop and refine these measures to ensure program success.

CBP's Records Management Practices for C-TPAT Are Inadequate

CBP's record keeping for the program is incomplete, as key decisions are not always documented and programmatic information is not updated regularly or accurately. Federal regulations require that bureau record-keeping procedures provide documentation to facilitate review by

Congress and other authorized agencies of government. Further, standards for internal control in the federal government require that all transactions be clearly documented in a manner that is complete, accurate, and useful to managers and others involved in evaluating operations.

To get a better understanding of the validation process, we asked CBP to provide us with examples of company files for which validations had been completed. CBP selected six members' files for us to review for some of the initial validations the bureau conducted. During our review, it was not always clear what aspect of the security profile was being validated and why a particular site was selected at which to conduct the validation because there was not always documentation of the decision-making process. The aspects of the security profiles covered and sites visited did not always appear to be the most relevant. For example, one validation report we reviewed for a major retailer—one that imports the vast majority of its goods from Asia—indicated that the validation team reviewed facilities in Central America. CBP officials noted that it recently revised its validation report format to better capture any justification for report recommendations and best practices identified. CBP then provided us with eight additional member files with more recently completed validation reports. After reviewing the more recent validation reports contained in these files, we noted that there appeared to be a greater discussion related to the rationale for validating specific aspects of the security profiles. However, these files did not consistently contain other documentation of members' application, certification, vetting, receipt of benefits, or validation. While files contained some of these elements, they were generally not complete. In fact, most files did not usually contain anything beyond copies of the member's C-TPAT agreement, security profiles, and validation report. When we asked if CBP required its supply chain specialists to document their communications with C-TPAT members, CBP officials told us there has been no requirement that communications be documented. For example, member files we reviewed contained no documentation of communications between CBP and members regarding how the scope of a validation was determined. Recently, supply chain specialists located at CBP headquarters (but not at field offices) have been asked to document all conversations with member companies on a spreadsheet, so that each supply chain specialist will be aware of the outcomes of conversations with member companies.

CBP does not update programmatic information regularly or accurately. In particular, the reliability of CBP's database to track member status using key dates in the application through validation processes is questionable. The database, which is primarily used for documentation management and

workflow tracking, is not updated on a regular basis. In addition, C-TPAT management told us that earlier data entered into the database may not be accurate, and CBP has taken no systematic look at the reliability of the database. CBP officials also told us that there are no written guidelines for who should enter information into the database or how frequently the database should be updated. We made several requests over a period of weeks to review the contents of the database to analyze workload factors, including the amount of time that each step in the C-TPAT application and review process was taking. The database information that CBP ultimately provided to us was incomplete, as many of the data fields were missing or inaccurate. For example, more than 33 percent of the entries for validation date were incomplete. In addition, data on the status of companies undergoing the validation process was provided in hard copy only and included no date information. CBP officials told us that they are currently exploring other data management systems, working to develop a new, single database that would capture pertinent data, as well as developing a paperless environment for the program.

Conclusions

CBP's primary reliance on members' self-reporting about their security procedures to receive C-TPAT benefits places added importance on the validation process, which is CBP's method of verifying the effectiveness, efficiency, and accuracy of the security profile. However, the weaknesses in the validation process we found raise questions about its effectiveness. CBP's validation process, the purpose of which is to ensure that members' security measures are reliable, accurate, and effective, is not rigorous enough to achieve CBP's goals because of the bureau's consideration of the process as a joint, partnership review with the member company. In this vein, without guidelines for what constitutes a validation, CBP cannot be sure that it effectively and consistently verifies a standard set of security measures to ensure some minimally appropriate level of vulnerability reduction, nor can it apply a methodical approach to assessing the security procedures. In addition, CBP has not assessed the extent (in terms of numbers or percentage) to which it must conduct validations to ensure that the C-TPAT program is consistent with its overall approach to managing risk. Also, we found a lack of clear documentation for the validation process. Because of these weaknesses, CBP's ability to provide assurance that the program prevents terrorists and terrorist weapons from entering the United States is limited.

Finally, CBP has not completed corrective actions from our July 2003 report, which were meant to change the management of the program from a short-term focus to a strategic focus. Specifically, CBP has not

completed (1) developing performance measures with which to measure the program's success in achieving bureau goals and inform decisions for process improvement and (2) developing a human capital plan to account for how the program will recruit, train, and retain staff to achieve program goals. CBP also does not have a basic records management system to ensure adequate internal controls to manage the program. Because of these management weaknesses, CBP will have difficulty effectively planning, executing, and monitoring the program.

Recommendations for Executive Action

To help CBP achieve C-TPAT objectives and address the challenges associated with its continued development, we recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to take the following five actions:

- strengthen the validation process by providing appropriate guidance to specialists conducting validations, including what level of review is adequate to determine whether member security practices are reliable, accurate, and effective;
- determine the extent (in terms of numbers or percentage) to which members should be validated in lieu of the original goal to validate all members within 3 years of certification;
- complete the development of performance measures, to include outcome-based measures and performance targets, to track the program's status in meeting its strategic goals;
- complete a human capital plan that clearly describes how the C-TPAT program will recruit, train, and retain sufficient staff to successfully conduct the work of the program, including reviewing security profiles, vetting, and conducting validations to mitigate program risk; and
- implement a records management system that accurately and timely documents key decisions and significant operational events, including a reliable system for (1) documenting and maintaining records of all decisions in the application through validation processes, including but not limited to documentation of the objectives, scope, methodologies, and limitations of validations, and (2) tracking member status.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of DHS for comment. We received comments from the Commissioner of U.S. Customs and Border Protection that are reprinted in appendix II. CBP generally agreed with our recommendations and outlined actions it either had taken or was planning to take to implement them.

CBP agreed with our two recommendations on validations and said it will readdress the validation process. Specifically, CBP said that it was developing standard operating procedures, guidance, and written baseline criteria for the validation process, as well as an automated validation tool to document validations. CBP also agreed to determine the extent to which C-TPAT members should be validated, stating that it will develop member selection criteria and an automated system to standardize and assist in the selection of companies for validation. If properly implemented, these actions should address the intent of these recommendations.

Our draft report also included a recommendation to complete a formal strategic plan that clearly articulates goals, linkages, and strategies. While our draft report was with DHS for comment, CBP issued its final strategic plan on January 13, 2005. Our brief review of this strategic plan indicates that it appears to address the intent of our recommendation. Therefore, we removed the recommendation from this report. Nevertheless, as CBP further refines its strategic plan in the future, we encourage CBP to include all of the key elements of a strategic plan as described in the Government Performance and Results Act of 1993. Specifically, the formal strategic plan should include a description of performance goals and how they are related to the general goals and objectives of the program, as well as a description of program evaluations, which are useful for identifying key factors likely to affect program performance.

CBP agreed with our recommendation on developing performance measures, and has developed initial measures relating to membership, inspection percentages, and validation effectiveness. CBP has developed new performance measures for use in the FY 2006 Fiscal Year Homeland Security Plan and plans to enlist the help of a contractor to develop other outcome-based performance measures and targets. If properly implemented, these plans should help address the intent of this recommendation.

In addressing our recommendation to complete a human capital plan for the C-TPAT program, CBP told us it is still developing an implementation plan for the program that will include those elements required in a human capital plan. For example, CBP said it has developed new positions, training programs and materials, and a staffing plan. Further, CBP said the C-TPAT program will continue to refine all aspects of its human capital plan to include headquarters personnel, additional training requirements, budget, and future personnel profiles. If the final implementation plan

contains these elements, the plan should address the intent of the recommendation.

CBP agreed with our recommendation on implementing a records management system that accurately and timely documents key decisions and significant operational events. While its comments did not specify the nature or capabilities of a new system, CBP indicated that in the near future, it plans to automate every aspect of the C-TPAT program, both internally and externally. In automating its system, to fully meet the intent of this recommendation, CBP needs to ensure that the system addresses all aspects of C-TPAT operations and that tracking member status is done timely, accurately, and reliably.

Notwithstanding its general agreement with the recommendations, CBP expressed some concerns regarding the report. In its general comments, CBP said that C-TPAT is a voluntary program that is not designed to confirm company compliance with regulatory requirements. Further, CBP said it is very difficult for the U.S. government to regulate supply chain security procedures outside the country. CBP also noted that it is looking to establish more broadly applicable minimum security standards that may build on C-TPAT requirements. Our report clearly notes that the program is of a voluntary nature, designed around security guidelines jointly developed by CBP and the trade community. The cooperation envisioned by the C-TPAT program can build productive relationships and encourage supply chain security. However, in accepting members into the program, CBP still has the responsibility for verifying that security measures planned or claimed by C-TPAT members are properly implemented and effective. This program goes beyond trade facilitation in that it awards benefits that can reduce the scrutiny given cargo containers arriving in the United States. This is not a matter of regulating supply chain security in other countries. Rather, it is a matter of providing a security benefit for containers arriving at our nation's ports. If CBP does not ensure that this important security-related benefit is deserved, it runs the risk of overlooking potentially dangerous cargo during the inspection process.

CBP also said that the report's title is misleading, asserting that it creates the improper impression that only the validation process ensures adequate security for containerized cargo and does not place enough emphasis on the certification and vetting processes, as well as omits that C-TPAT cargo is not exempt from advance reporting requirements or enforcement and security inspections, such as random inspections and nonintrusive screening technology. Our report clearly describes the various steps CBP takes in the overall cargo inspection process and how the C-TPAT

program fits into that process. The report also clearly describes the purpose of each process within the C-TPAT program, including the validation process that is to determine whether C-TPAT members' security procedures are accurate, reliable, and effective. We did modify the report's title and, where appropriate, the text to better reflect the report's focus on C-TPAT versus other programs in CBP's layered enforcement strategy for cargo security. However, any weakness in C-TPAT could weaken CBP's layered approach. Given that C-TPAT members enjoy benefits that reduce the likelihood of an inspection of their cargo, not having an effective validation process could serve to defeat the purposes of the other enforcement layers.

Finally, CBP noted many benefits achieved under the C-TPAT program, including that thousands of companies working as part of C-TPAT have taken concrete steps to improve their security procedures and that C-TPAT has fostered an expanding international dialogue on best security practices. We agree that actions on the part of program members to shore up supply chain security are valuable and desirable. Again, with the threat of terrorism present in the global supply chain, we believe that verifying that planned improvements are actually implemented and ensuring that security controls are effective are important responsibilities that cannot be achieved only with members self-reporting about their security procedures.

CBP also offered technical comments and clarifications, which we considered and incorporated where appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies of this report to appropriate departments and interested congressional committees. We will also make copies available to others upon request. In addition, the report will be available on GAO's Web site http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or at stanar@gao.gov. Key contributors to this report are listed in appendix III.

Richard M. Stana

Richard M. Stana
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

We addressed the following questions regarding the U.S. Customs and Border Protection's (CBP, formerly the U.S. Customs Service) Customs-Trade Partnership Against Terrorism (C-TPAT):

- What benefits does CBP provide to C-TPAT members?
- Before providing benefits, what approach does CBP take to determine C-TPAT members' eligibility for them?
- After providing benefits, how does CBP verify that members have implemented their security measures?
- To what extent has CBP developed strategies and related management tools for achieving the program's goals?

Scope and Methodology

To address these questions, we visited CBP's headquarters in Washington, D.C., which manages the C-TPAT program. We interviewed CBP officials and reviewed available data and documentation for the program. We reviewed individual CBP files for a subset of C-TPAT members, including members with responsibilities along various parts of the supply chain. We also reviewed CBP's database for tracking member status in the program from the program's inception through July 2004. All records in this database were reviewed. We intended to use these data to select a random set of files to review and to conduct analyses of workloads, but the data were not reliable enough to do so (see below). Given the weaknesses in the files as well as the data reliability issues, our review focused on identifying C-TPAT's processes. Because of deficiencies in the files and database, we were unable to verify the extent CBP actually follows these processes for individual members. We also obtained the status of the agency's efforts to implement our prior recommendations for the program, including the completion of a strategic plan, a human capital plan, and performance measures.

We conducted our work from February through December 2004 in accordance with generally accepted government auditing standards.

Data Reliability

To assess the reliability of CBP's database for tracking member status in C-TPAT, we (1) reviewed existing documentation related to the data sources, (2) electronically tested the data to identify obvious problems with completeness or accuracy, and (3) interviewed knowledgeable bureau officials about the data. Initial reliability testing of this database and interviews of staff with responsibility for the program led us to conclude that data used to track participant status had some serious reliability weaknesses. We determined that using the data in certain cases, for example, to calculate average times for phases of the membership

process, might have led to an incorrect or misleading message. However, we determined that the data were sufficiently reliable for limited use in descriptions of the program status, such as the approximate numbers of participants, because our analysis and discussions with CBP officials assured us that those data fields were reasonably complete and accurate.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

Commissioner

Mr. Richard M. Stana
Director, Homeland Security and Justice
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Stana:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report related to the Customs-Trade Partnership Against Terrorism (C-TPAT) program. U.S. Customs and Border Protection (CBP) and the Department of Homeland Security (DHS) appreciate the work done in this review to identify areas where actions can be taken by CBP to improve the C-TPAT program. Technical comments were provided to GAO under a separate cover; however, there are a few areas of the report that deserve comment.

When C-TPAT was established in response to the attacks of September 11, the intent was to build a partnership to leverage the resources of the private sector so that the limited resources of the government could be focused on inspecting high-risk cargo shipments. Any evaluation of C-TPAT must recognize that it is a voluntary partnership to improve the security of the United States and not a program to confirm importer compliance with a regulatory requirement. The C-TPAT participants voluntarily share with the government details of sensitive corporate security plans and again, voluntarily, agree to allow government representatives access to their facilities to confirm that they are following their own security plans and that these plans meet or exceed C-TPAT supply chain security criteria. DHS believes that to date, thousands of companies working under the auspices of this partnership have taken concrete steps to improve their security procedures, thereby increasing global supply chain security and the security of the United States.

The supply chain that facilitates the shipment of cargo to the United States is global. It is very difficult for our government to regulate the security procedures outside our country. However, C-TPAT importers are willing to use their business leverage over their foreign suppliers throughout the world to require their suppliers to improve security at the beginning of the supply chain.

This free and open communication with industry has allowed Customs and Border Protection to further identify security baseline practices and best practices. This has been a learning experience for all involved, and through this exchange C-TPAT has

2

fostered an expanding international dialogue on best security practices. This has created an opportunity for DHS to work internationally to promote supply chain security.

C-TPAT is a partnership program that has benefits for both the government and the industry participants. The title of the draft report, "DHS Grants Importers Reduced Scrutiny with Limited Assurance of Adequate Security", is misleading. The title creates the improper impression that only the validation process assures adequate security for containerized cargo. The report places excessive emphasis on the validation process without adequately reflecting the certification and vetting process within C-TPAT and the other layers of security put in place since the terrorist attacks three years ago. However, as noted below, we believe the shipments of a company which has committed to C-TPAT security levels represent less risk. That lessened risk is taken into account in our risk targeting rules. That said, C-TPAT cargo is not exempt from advance reporting requirements, enforcement and security inspections, random inspections, or non-intrusive screening technology such as radiation portals where we are moving to 100% screening of all in-bound cargo for WMD threats. The DHS cargo security strategy clearly identifies the screening of all containers for WMD's as its highest priority.

The discussion of the benefits of C-TPAT, including the section "C-TPAT Benefits Designed to Reduce Scrutiny of Shipments" would be more accurate if it reflected that the benefits of the program were designed to create incentives for industry to improve supply chain security. Eligibility for the Importer Self-Assessment Program (ISA) for example, is included as a benefit that reduces the level of scrutiny.

Further, CBP, in the context of the DHS cargo security strategy, is looking to establish more broadly applicable minimum security standards that may in some cases build on C-TPAT requirements. For example, CBP is currently working on a proposed regulatory standard that would require 100 percent of all loaded in-bound maritime containers to be outfitted with a high-security seal that would be verified before the cargo is loaded at the foreign port. The C-TPAT program currently includes guidelines for high security seals that meet or exceed this regulatory requirement. The movement of a C-TPAT guideline to a more broadly regulated minimum standard is another way to transition industry towards a stricter security framework.

Finally, C-TPAT is part of our overall risk management approach. C-TPAT helps identify the importers that take security seriously. This information is factored into the risk assessment and lower risk cargo receives less scrutiny. That is how risk management works. The resources used to validate that low risk importers are truly low risk must be reasonable when balanced against the greater threat presented by higher risk cargo. That is not to say that the C-TPAT program cannot be improved. On the contrary, DHS concurs with the final recommendations in the report.

As part of their corrective action plan, CBP will readdress the validation process, including establishing policies and procedures related to the extent to which C-TPAT

3

members are validated. Actions that CBP plans to take regarding specific recommendations are below:

Recommendation 1: Strengthen the validation process by providing appropriate guidance to specialists conducting validations, including what level of review is adequate to determine whether member security practices are reliable, accurate, and effective.

Response: CBP has provided all Supply Chain Specialists (SCS) with a comprehensive training program developed by CBP's Office of Training and Development. SCS training includes specific instruction on validation scope and methodology, conducting pre-validation research, supply chain identification/selection, and report writing. CBP is developing Standard Operating Procedures and directives to provide further clarification and guidance for all SCS personnel conducting validations. This will include the need for appropriate documentation of the validation process. CBP will also develop an automated validation tool for SCS.

Recognizing that no two international supply chains or validations are exactly the same, and that C-TPAT must remain flexible to meet the complex challenges of international trade, CBP will develop written baseline criteria for assisting the SCS in determining if member's security practices and processes are adequate and effective.

Recommendation 2: Determine the extent (in terms of numbers or percentage) to which members should be validated in lieu of the original goal to validate all members within three years of certification.

Response: Overwhelming response by the trade community forced CBP to reconsider its original goal to validate all certified members within a three-year period. Selection for validations were initially based upon risk management principles, i.e., strategic threat geographically, import volume/value, security related incidents, history of compliance/violations, etc. CBP will further refine the risk management process and develop member selection methodology/criteria and an automated system to standardize and assist in the selection process. C-TPAT will determine and prioritize which sectors of membership will be selected for validations, select individual companies based upon a standardized risk assessment, and identify "company specific" high-risk supply chains to better focus our efforts and resources. The resource needs to support this approach will be reflected in the human capital plan.

Recommendation 3: Complete a formal strategic plan that clearly articulates the goals of the C-TPAT program, their relationship to broader CBP goals, and strategies for achieving them.

Response: As part of its ongoing industry outreach effort, C-TPAT has developed a strategic plan that was shared with the public during CBP's Trade Symposium on January 13 and 14, 2005 and is attached to this response. CBP is continuing its efforts to strategically strengthen C-TPAT and is working with the Department of Homeland Security to draft an implementation plan for the program. This implementation plan will

4

build on the public dialogue associated with the strategic plan and specifically focus on developing performance metrics to adequately assess security and trade facilitation aspects, human resource requirements and a plan for transitioning C-TPAT requirements to minimum baseline standards (as may be appropriate), consistent with GAO's recommendations."

Recommendation 4: Complete the development of performance measures, to include outcome-based measures and performance targets, to track the program's status in meeting its strategic goals.

Response: C-TPAT has developed initial measures to determine the scope of the program (i.e., membership), measures to gauge the realization of benefits by certified members (i.e., inspection percentages), and measures to gauge the effectiveness of validations. C-TPAT has refined its measures in coordination with the Department. New measures have been developed for use in the FY 2006 Fiscal Year Homeland Security Plan. They include: compliance rate for C-TPAT members with the established C-TPAT security guidelines, C-TPAT validation labor efficiency rate, average CBP exam reduction ratio for C-TPAT member importers compared to non-C-TPAT importers, and time savings to process U.S./Mexico Border FAST lane transactions. In addition, CBP will be identifying a contractor to assist with the development of outcome-based measures and performance targets for the C-TPAT program. CBP will continue to develop and refine these and other measures as may be required to ensure program success.

Recommendation 5: Complete a formal human capital plan that clearly describes how the C-TPAT program will recruit, train, and retain sufficient staff to successfully conduct the work of the program, including reviewing security profiles, vetting, and conducting validations to mitigate program risk.

Response: To date, C-TPAT has developed the new SCS position, developed an official 2 week training program, developed a formalized SCS training manual, conducted two rounds of SCS selections, conducted two formal training programs, established four C-TPAT field offices, and developed a future continuing education program for C-TPAT personnel. In addition, CBP produced a detailed SCS staffing plan which analyzed current SCS workload, annual program growth rate, actual duties being performed by SCS, time to complete average validation, and the number of validations an SCS can complete in 1 year. C-TPAT will continue to refine all aspects of the human capital plan to include Headquarters personnel, additional training requirements, budget, and future personnel profiles.

Recommendation 6: Implement a records management system that accurately and timely documents key decisions and significant operational events, including a reliable system for (1) documenting and maintaining records of all decisions in the application through validation processes, including but not limited to documentation of the objectives, scope, methodologies, and limitation of validations, and (2) tracking member status.

This version of our report is unrestricted based on a security review by CBP.

5

Response: CBP's goal is to automate every aspect of the C-TPAT program, both internally and externally. In the near future, only electronic submissions will be accepted by C-TPAT. Trade partners will submit information through a web application. The information will be processed against internal risk criteria and accepted or denied immediate responses generated and validation time frames established. Internally, information will be easily stored, reports generated and risk analysis conducted. Externally, response times will decrease and more information will be readily available.

Thank you for the opportunity to review and provide comments to the draft report. Our expectation is that this report will be handled appropriately as a "Limited Official Use Only" document due to the sensitivity of the information contained in the report.

Yours truly,

Robert C. Bonner
Commissioner

Attachment

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Richard M. Stana (202) 512-8777
Stephen L. Caldwell (202) 512-9610

Staff Acknowledgments

In addition to those named above, Kristy N. Brown, Kathryn E. Godfrey, Wilfred B. Holloway, Stanley J. Kostyla, Shakira O'Neil, and Deena D. Richart made key contributions to this report.

Related GAO Products

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

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

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO-04-1062. Washington, D.C.: September 30, 2004.

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

Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands. GAO-04-590. Washington, D.C.: June 2004.

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

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T. Washington, D.C.: March 23, 2004.

Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information. GAO-04-319R. Washington, D.C.: December 18, 2003.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T. Washington, D.C.: December 16, 2003.

Posthearing Questions Related to Aviation and Port Security. GAO-04-315R. Washington, D.C.: December 12, 2003.

Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. GAO-03-1083. Washington, D.C.: September 19, 2003.

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T. Washington, D.C.: September 9, 2003.

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

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions. GAO-03-902T. Washington, D.C.: June 16, 2003.

Transportation Security: Federal Action Needed to Address Security Challenges. GAO-03-843. Washington, D.C.: June 30, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Border Security: Challenges in Implementing Border Technology. GAO-03-546T. Washington, D.C.: March 12, 2003.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2005

CONTAINER SECURITY

A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts

GAO
Accountability * Integrity * Reliability

GAO-05-557

Permanent Subcommittee on Investigations
EXHIBIT #9

GAO
Accountability-Integrity-Reliability
Highlights

Highlights of GAO-05-557, a report to congressional requesters

Why GAO Did This Study

In January 2002, U.S. Customs and Border Protection (CBP) initiated the Container Security Initiative (CSI) to address the threat that terrorists might use maritime cargo containers to ship weapons of mass destruction. Under CSI, CBP is to target and inspect high-risk cargo shipments at foreign seaports before they leave for destinations in the United States. In July 2003, GAO reported that CSI had management challenges that limited its effectiveness. Given these challenges and in light of plans to expand the program, GAO examined selected aspects of the program's operation, including the (1) factors that affect CBP's ability to target shipments at foreign seaports, (2) extent to which high-risk containers have actually been inspected overseas, and (3) extent to which CBP formulated and documented strategies for achieving the program's goals.

What GAO Recommends

GAO recommends that CBP refine its staffing model to help improve the program's ability to target shipments at foreign ports, develop minimum technical requirements for the detection capabilities of equipment used in the program, and complete development of performance measures for all program objectives.

The Department of Homeland Security (DHS) generally concurred with our recommendations and described corrective actions to respond to them. The Department of State had no comments.

www.gao.gov/cgi-bin/getrpt?GAO-05-557. To view the full product, including the scope and methodology, click on the link above. For more information, contact Richard M. Stana at (202) 512-8777 or stanar@gao.gov.

April 2005

CONTAINER SECURITY

A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts

What GAO Found

Some of the positive factors that have affected CBP's ability to target shipments overseas are improved information sharing between U.S. and foreign customs staff and a heightened level of bilateral cooperation and international awareness of the need to secure the whole global shipping system. Although the program aims to target all U.S.-bound shipments from CSI ports, it has been unable to do so because of staffing imbalances. CBP has developed a staffing model to determine staffing needs but has been unable to fully staff some ports because of diplomatic considerations (e.g., the need for host government permission) and practical considerations (e.g., workspace constraints). As a result, 35 percent of these shipments were not targeted and were therefore not subject to inspection overseas. In addition, the staffing model's reliance on placing staff at CSI ports rather than considering whether some of the targeting functions could be performed in the United States limits the program's operational efficiency and effectiveness.

CBP has not established minimum technical requirements for the detection capability of nonintrusive inspection and radiation detection equipment used as part of CSI. Ports participating in CSI use various types of nonintrusive inspection equipment to inspect containers, and the detection and identification capabilities of such equipment can vary. In addition, technologies to detect other weapons of mass destruction have limitations. Given these conditions, CBP has limited assurance that inspections conducted under CSI are effective at detecting and identifying terrorist weapons of mass destruction.

Although CBP has made some improvements in the management of CSI, we found that further refinements to the bureau's management tools are needed to help achieve program objectives. In July 2003, we recommended that CBP develop a strategic plan and performance measures, including outcome-oriented measures, for CSI. CBP developed a strategic plan for CSI in February 2004 that contains three of the six key elements required for agency strategic plans, and CBP officials told us they continue to develop the other three elements. While it appears that the bureau's efforts in this area meet the intent of our prior recommendation to develop a strategic plan for CSI, we will continue to monitor progress in this area. CBP has also made progress in the development of outcome-oriented performance measures, particularly for the program objective of increasing information sharing and collaboration among CSI and host country personnel. However, CBP continues to face challenges in developing performance measures to assess the effectiveness of CSI targeting and inspection activities. Therefore, it is difficult to assess progress made in CSI operations over time, and it is difficult to compare CSI operations across ports.

Contents

Letter		1
	Results in Brief	4
	Background	5
	While CBP Has Enhanced Its Ability to Target Containers Overseas, Limitations Remain	17
	Some Containers Not Inspected for a Variety of Reasons	21
	CBP Has Made Progress Developing a Strategic Plan and Performance Measures for CSI, but Further Refinements Are Needed	26
	Conclusions	33
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	34
Appendix I	**Objectives, Scope, and Methodology**	36
	Objectives	36
	Scope and Methodology	36
	Data Reliability	37
Appendix II	**CSI Performance Measures, as of January 2005**	39
Appendix III	**Comments from the Department of Homeland Security**	42
Appendix IV	**GAO Contacts and Staff Acknowledgments**	44
	GAO Contacts	44
	Staff Acknowledgments	44
Related GAO Products		45
Tables		
	Table 1: CSI Operational Seaports, as of February 2005	12
	Table 2: CSI Outcome-Oriented Performance Measures	30

Figures

Figure 1: CBP's Domestic Process for Targeting and Inspecting Cargo Containers 9
Figure 2: Commercial Sample Image Produced by an X-ray Imaging Machine of a Cargo Container Loaded on a Truck Trailer 10
Figure 3: CSI Process for Targeting and Inspecting Cargo Containers Overseas 15

Abbreviations

ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
GPRA	Government Performance and Results Act of 1993
ICE	U.S. Immigration and Customs Enforcement
NTC	National Targeting Center
OMB	Office of Management and Budget
PRD	personal radiation detector
RIID	radiation isotope identifier device
RPM	radiation portal monitor
WCO	World Customs Organization
WMD	weapons of mass destruction

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

United States Government Accountability Office
Washington, DC 20548

April 26, 2005

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

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

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Ocean cargo containers play a vital role in the movement of cargo between global trading partners. In 2004, nearly 9 million ocean cargo containers arrived and were offloaded at U.S. seaports. Responding to heightened concern about national security since September 11, 2001, several U.S. government agencies have focused efforts on preventing terrorists from smuggling weapons of mass destruction (WMD) in cargo containers from overseas locations to attack the United States and disrupt international trade.[1] Because of its frontline responsibilities for inspection at U.S. ports of entry, the U.S. Customs and Border Protection (CBP) has the lead U.S.

[1]Throughout this report, we use the term *weapons of mass destruction* to refer to chemical, biological, radiological, or nuclear agents or weapons. Some agencies define *WMD* to include large conventional explosives as well. Another term being used almost synonymously with WMD is *weapons of mass effect*, which refers to a terrorist attack that would not explicitly fit this definition of WMD. As clearly demonstrated by the events of September 11, a terrorist attack would not have to fit the definition of WMD to achieve mass effect in terms of mass casualties, destruction of critical infrastructure, economic losses, and disruption of daily life nationwide.

role in ensuring ocean container security and reducing the vulnerabilities associated with the overseas supply chain.

In light of the complexity and interconnectedness of global commerce, international cooperation is a key factor in reducing the vulnerability of oceangoing cargo. To help address its responsibility to ensure the security of this cargo, CBP has in place a program known as the Container Security Initiative (CSI). The program aims to target and inspect high-risk cargo shipments at foreign seaports before they leave for destinations in the United States. Under the program, foreign governments agree to allow CBP personnel to be stationed at foreign seaports to use intelligence and automated risk assessment information to target shipments to identify those at risk of containing WMD or other terrorist contraband. CBP personnel are to refer these high-risk shipments to host government officials, who are then to determine whether to inspect the shipment before it leaves the port for the United States. Host government officials examine shipments with nonintrusive inspection equipment (such as X-ray machines) and, if they deem it necessary, open the cargo containers to physically examine the contents inside. As of February 2005, the CSI program was operational at 34 foreign seaports, with plans to expand to an additional 11 ports by the end of fiscal year 2005.

The program is promising, but our previous work has raised concerns about its management and its ability to achieve its ultimate goal of improved cargo security. In July 2003, we reported that CBP's management of CSI had not evolved from a short-term focus to a long-term strategic approach.[2] We recommended that the Secretary of the Department of Homeland Security (DHS) work with the Commissioner of U.S. Customs and Border Protection to develop (1) a strategic plan that clearly lays out the program's goals, objectives, and detailed implementation strategies; (2) performance measures that include outcome-oriented indicators; and (3) a human capital plan that clearly describes how CSI will recruit, train, and retain staff to meet the program's growing demands as the bureau implements new program elements. In March 2004, we testified that CBP's targeting system does not incorporate all key elements of a risk management framework and recognized

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

modeling practices in assessing the risks posed by oceangoing cargo containers.[3]

In light of the program's planned expansion, we examined selected aspects of the program's operation and management. This report addresses the following issues:

1. What factors affect CBP's ability to target shipments at overseas seaports?

2. Under CSI, to what extent have high-risk containers been inspected overseas prior to their arrival at U.S. destinations?

3. To what extent has CBP developed strategies and related management tools for achieving the program's goals?

To address all three objectives, we met with CBP officials in Washington, D.C., who have program responsibilities for CSI and reviewed available data and documentation for the program. To ascertain the degree to which high-risk shipments were targeted and inspected overseas, we obtained data on CSI targeting and inspection activity for each of the CSI ports. We also met with CSI teams and host government officials at four overseas ports. In addition, we observed elements of the targeting and inspection processes at these ports and obtained and reviewed documentation of CSI procedures provided by CBP and host government officials at these ports. We also assessed the reliability of CBP's data on the number of shipments and containers subject to targeting and inspection under CSI and found the data sufficiently reliable for use in our report. In addition, we examined the status of the bureau's efforts to implement our prior recommendations for strategic and human capital plans and performance measures for the program.

We conducted our work from February 2004 through February 2005 in accordance with generally accepted government auditing standards. More details about the scope and methodology of our work are presented in appendix I.

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

Results in Brief

We identified both positive and negative factors that affect CBP's ability to target shipments at overseas seaports. According to CBP officials, some of the positive factors are improved information sharing between U.S. and foreign customs operations and a heightened level of bilateral cooperation and international awareness regarding securing the whole global shipping system across governments. Related to these factors, as of February 2005 CBP had successfully negotiated agreements with host nations to allow CSI to operate in 34 foreign seaports. As of September 11, 2004, CSI teams were able to target approximately 65 percent of the U.S.-bound shipments coming through CSI ports to determine whether they were high-risk and should be referred to host government customs officials for inspection. This represents about 43 percent of all shipments transported to the United States by oceangoing cargo containers. However, other, negative factors limit CBP's ability to successfully target containers to determine if they are high-risk. One such factor is staffing imbalances, which impede CBP from targeting all containers shipped from CSI ports before they leave for the United States. While CBP has developed a staffing model to determine the required level of staff, political and practical considerations have limited the number of staff at some ports. As a result of these imbalances, 35 percent of U.S.-bound shipments from CSI ports were not targeted and were therefore not subject to inspection overseas—the key goal of the CSI program. One of the features of the CSI staffing model that may contribute to the staffing imbalance is its reliance on placing staff overseas at CSI ports. Another negative factor is weaknesses in manifest data, one source of data used for targeting shipments.

As of September 11, 2004, host government officials inspected the majority of containers referred to them for inspection by CSI teams. However, 28 percent of these containers were not inspected for a variety of reasons. For example, 1 percent of the container referrals were denied by host government officials, generally because they believed the referrals were based on factors not related to security threats, such as drug smuggling. For referred containers that are not inspected by host governments overseas, the CSI team is supposed to refer the container for inspection by CBP upon arrival at the U.S. destination port. Although CBP officials did not have information going back to the inception of CSI, they noted that between July 2004 and September 2004, about 93 percent of shipments referred for domestic inspection were inspected at a U.S. port. CBP explained that some referred shipments were not inspected domestically because inspectors at U.S. ports received additional intelligence information that lowered the risk characterization of the shipments or because the shipments remained aboard the carrier while in the U.S. port. For the 72 percent of referred containers that were inspected overseas,

CBP officials told us that no WMD were discovered. However, the inspection equipment used at CSI ports varies in detection capability and there are no minimum technical requirements for equipment used as part of CSI. In addition, technologies to detect other WMD have limitations. As a result, CBP has limited assurance that inspections conducted under CSI are effective at detecting and identifying terrorist WMD in containers.

Although CBP has made some improvements in the management of CSI, we found that further refinements to the bureau's management tools are needed to help achieve program goals. In July 2003, we recommended that CBP develop a strategic plan and performance measures, including outcome-oriented measures, for CSI. CBP issued a strategic plan for CSI in February 2004 that contains three of the six key elements required for agency strategic plans: a mission statement, long-term objectives, and implementation strategies. The director of CBP's Strategic Planning and Audit Division told us the bureau continues to develop the other three elements for the CSI strategic plan: (1) describing how performance goals are related to general goals of the program, (2) identifying key external factors that could affect program goals, and (3) describing how programs are to be evaluated. CBP has also made progress in the development of outcome-oriented performance measures, particularly for the program objective of increasing information sharing and collaboration among CSI and host country personnel. However, CBP continues to face challenges in developing performance measures to assess the effectiveness of CSI targeting and inspection activities. Therefore, it is difficult to assess progress made in CSI operations over time, and it is difficult to compare CSI operations across ports.

We are making several recommendations to improve the program's ability to meet its objectives. These include revising its staffing model, developing minimum detection capability requirements for nonintrusive inspection equipment used in the program, and completing development of performance measures for all program objectives. We provided a draft of this report to the Secretary of DHS and the Department of State for comment. In its response, DHS noted that CBP generally agreed with our recommendations and cited corrective actions it either has taken or planned to take. The Department of State had no comments on the draft report.

Background

Several studies on maritime security conducted by federal, academic, nonprofit, and business organizations have concluded that the movement of oceangoing cargo in containers is vulnerable to some form of terrorist action, largely because of the movement of shipments throughout the

supply chain.[4] Relatively few importers own and operate all key aspects of the cargo container transportation process, which includes overseas manufacturing and warehouse facilities, carrier ships to transport goods, and the transportation operation to receive the goods upon arrival. Most importers must rely on second-hand parties to move cargo in containers and prepare various transportation documents. Second-hand parties within the cargo container supply chain may include exporters, freight forwarders, customs brokers, inland transportation providers, port operators, and ocean carriers. Every time responsibility for cargo in containers changes hands along the supply chain, there is the potential for a security breach; specifically, this change in responsibility creates opportunities for contraband to be placed in containers and opportunities for fraudulent documents to be prepared. According to the U.S. Department of Transportation's Volpe National Transportation Systems Center, importers who own and operate all aspects of the supply chain suffer the fewest security breaches because of their increased level of control.[5]

While CBP has noted that the likelihood of terrorists smuggling WMD into the United States in cargo containers is low, the nation's vulnerability to this activity and the consequence of such a disaster are high. With about 90 percent of the world's maritime cargo moving by containers, terrorist action related to cargo containers could paralyze the maritime trading system and quickly disrupt U.S. and global commerce. In a strategic simulation of a terrorist attack sponsored by the consulting firm Booz Allen Hamilton in 2002, representatives from government and industry organizations participated in a scenario involving terrorist activities at U.S. seaports.[6] The scenario simulated the discovery and subsequent detonation of "dirty bombs"—explosive devices wrapped in radioactive material and designed to disperse radiological contamination—hidden in cargo containers at various locations around the country. These "events" led simulation participants to shut down every seaport in the United States

[4]The supply chain consists of all stages involved, directly or indirectly, in fulfilling a customer request. These include the manufacturer, suppliers, transporters, warehouses, retailers, and customers. A supply chain involves the flow of information, product, and funds between the different stages.

[5]Department of Transportation, Volpe National Transportation Systems Center, *Intermodal Cargo Transportation: Industry Best Security Practices* (Cambridge, Mass.: June 2002).

[6]Mark Gerencser, Jim Weinberg, and Don Vincent, *Port Security Wargame: Implications for U.S. Supply Chains*, (Booz Allen Hamilton, October 2002).

over a period of 12 days. Booz Allen Hamilton published a report in October 2002 about the results of the simulation, which estimated that the 12-day closure would result in a loss of $58 billion in revenue to the United States' economy, including spoilage, loss of sales, manufacturing slowdowns, and halts in production. Further, according to the report, it would take 52 days to clear the resulting backlog of vessels and 92 days to stabilize the container backlog, causing a significant disruption in the movement of international trade.

CBP's Targeting and Inspection Approach at Domestic Ports

According to CBP, the large volume of imports and the bureau's limited resources make it impractical to inspect all oceangoing containers without disrupting the flow of commerce. CBP also noted it is unrealistic to expect that all containers warrant such inspection because each container poses a different level of risk based on a number of factors including the exporter, the transportation providers, and the importer. CBP has implemented an approach to container security that attempts to focus resources on particularly risky cargo while allowing other cargo to proceed.

CBP's domestic efforts to target cargo to determine the risk it poses rely on intelligence, historical trends, and data provided by ocean carriers and importers. Pursuant to federal law, CBP requires ocean carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before the cargo is loaded on a ship at a foreign port.[7] This information is used by CBP's Automated Targeting System (ATS). ATS is characterized by CBP as a rule-based expert system that serves as a decision support tool to assess the risk of sea cargo.[8] In addition, CBP requires importers to provide entry-level data that are entered into the Automated Commercial System and also used by ATS. According to CBP

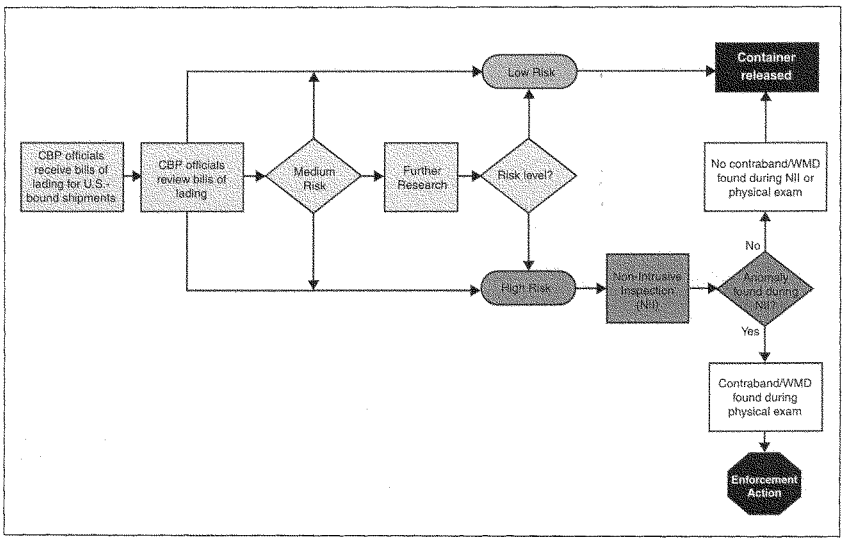
[7]Cargo manifest transmission requirements are located in regulations promulgated under Section 343 of the Trade Act of 2002, Public Law 107-210, as amended by Section 108 of the Maritime Transportation Security Act, Public Law 107-295. Cargo manifests are composed of bills of lading for each shipment laden on a vessel. A bill of lading includes the name of the shipping line, importer, consignee (recipient of the shipment), and manufacturer. The bill of lading also identifies the commodity being shipped, the date the shipment was sent, the number of containers used to transport the shipment, the port where the containers were laden on the U.S.-bound vessel, and the country from which the shipment originated.

[8]An expert system is a model that can chain together input data and intercept queries in order to make inferences.

officials, ATS uses this information to screen all containers to determine whether they pose a risk of containing WMD.

As shown in figure 1, CBP targeters at domestic ports target containers by first accessing the bills of lading and their associated risk scores electronically. The assigned risk score helps the targeters determine the risk characterization of a container and the extent of documentary review or inspection that will be conducted. For example, containers characterized as high-risk are to be inspected. Containers characterized as medium-risk are to be further researched. That is, targeters are to consider intelligence alerts and research assistance provided by the National Targeting Center (NTC) to the ports, and their own experience and intuition, in characterizing the final risk of shipments. Containers characterized as low-risk are generally to be released from the port without further documentary review or inspection.

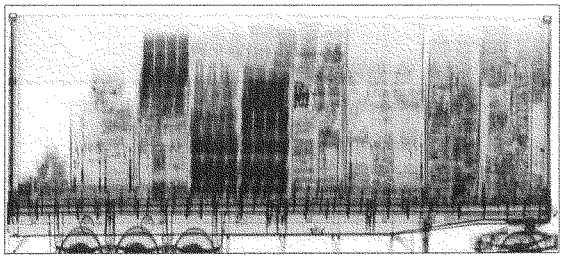
Figure 1: CBP's Domestic Process for Targeting and Inspecting Cargo Containers



Source: U.S. Customs and Border Protection.

There are, generally, two types of inspections that CBP inspectors may employ when examining cargo containers—nonintrusive inspections and physical examinations. The nonintrusive inspection, at a minimum, involves the use of X-ray or gamma-ray scanning equipment. As shown in figure 2, the X-ray or gamma ray equipment is supposed to scan a container and generate an image of its contents. CBP inspectors are to review the image to detect any anomalies, such as if the density of the contents of the container is not consistent with the description of the contents.

Figure 2: Commercial Sample Image Produced by an X-ray Imaging Machine of a Cargo Container Loaded on a Truck Trailer



Source: Host government customs organizations.

If an anomaly is apparent in the image of the container, CBP inspectors are to decide whether to conduct a physical examination of the container. According to CBP officials, they have a policy to determine the type of physical examination to be conducted depending on the location of the anomaly.

CBP inspectors also are to use radiation detection devices to detect the presence of radioactive or nuclear material. If the detectors indicate the presence of radioactive material, CBP officials are to isolate the source and contact the appropriate agency, such as the Department of Energy, for further guidance.

CBP Extended Its Targeting and Inspection Activities to Overseas Seaports

Announced in January 2002, CSI was implemented to allow CBP officials to target containers at overseas seaports so that any high-risk containers may be inspected prior to their departure for U.S. destinations. According to the CSI strategic plan, strategic objectives for CSI include (1) pushing the United States' zone of security beyond its physical borders to deter and combat the threat of terrorism; (2) targeting shipments for potential terrorists and terrorist weapons, through advanced and enhanced information and intelligence collection and analysis, and preventing those shipments from entering the United States; (3) enhancing homeland and border security while facilitating growth and economic development within the international trade community; and (4) utilizing available technologies to leverage resources and to conduct examinations of all containers posing a high risk for terrorist related activity. Another

objective cited by CBP officials, although not included in the CSI strategic plan, is to raise the level of bilateral cooperation and international awareness regarding the need to secure global trade.

To implement CSI, CBP negotiates and enters into bilateral arrangements with foreign governments, specifying the placement of CBP officials at foreign ports and the exchange of information between CBP and foreign customs administrations. CBP first solicited the participation of the 20 foreign ports that shipped the highest volume of ocean containers to the United States. These top 20 ports are located in 14 countries and regions and shipped a total of 66 percent of all containers that arrived in U.S. seaports in 2001. CBP has since expanded CSI to strategic ports, which may ship lesser amounts of cargo to the United States but may also have terrorism or geographical concerns. As shown in table 1, as of February 2005, CSI was operational at 34 ports, located in 17 countries or regions. For fiscal year 2004, the CSI budget was about $62 million, with a budget of about $126 million in fiscal year 2005 for the program.

Table 1: CSI Operational Seaports, as of February 2005

Country/region	CSI port	Date CSI operations began at port
Canada	Halifax	March 2002
	Montreal	March 2002
	Vancouver	February 2002
The Netherlands	Rotterdam	September 2002
France	Le Havre	December 2002
	Marseilles	January 2005
Germany	Bremerhaven	February 2003
	Hamburg	February 2003
Belgium	Antwerp	February 2003
	Zeebrugge	October 2004
Republic of Singapore	Singapore	March 2003
Japan	Yokohama	March 2003
	Tokyo	May 2004
	Nagoya	August 2004
	Kobe	August 2004
Hong Kong Special Administrative Region of China	Hong Kong	May 2003
Sweden	Gothenburg	May 2003
United Kingdom	Felixstowe	May 2003
	Liverpool	October 2004
	Southampton	October 2004
	Thamesport	October 2004
	Tilbury	October 2004
Italy	Genoa	June 2003
	La Spezia	June 2003
	Livorno	December 2004
	Naples	September 2004
	Gioia Tauro	October 2004
South Korea	Busan	August 2003
South Africa	Durban	December 2003
Malaysia	Port Klang	March 2004
	Tanjung Pelepas	August 2004
Greece	Piraeus	July 2004
Spain	Algeciras	July 2004
Thailand	Laem Chabang	August 2004

Source: CBP.

To participate in CSI, a host nation must meet several criteria. The host nation must utilize (1) a seaport that has regular, direct and substantial container traffic to ports in the United States; (2) customs staff with the authority and capability of inspecting cargo originating in or transiting through its country; and (3) nonintrusive inspection equipment with gamma- or X-ray capabilities and radiation detection equipment. Additionally, each potential CSI port must indicate a commitment to (1) establishing an automated risk management system; (2) sharing critical data, intelligence, and risk management information with CBP officials; (3) conducting a thorough port assessment to ascertain vulnerable links in a port's infrastructure and commit to resolving those vulnerabilities; and (4) maintaining a program to prevent, identify, and combat breaches in employee integrity.

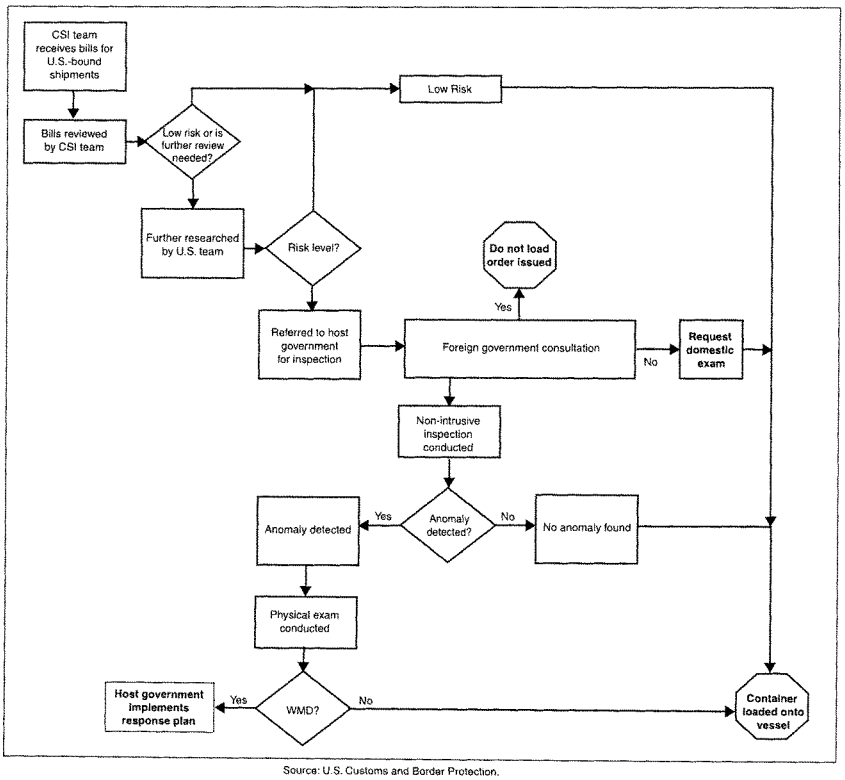
To prepare for implementation of CSI, CBP sends an assessment team to each potential CSI port to collect information about the port's physical and information infrastructure, the host country's customs operations, and the port's strategic significance to the United States. CBP then deploys a CSI team, which generally consists of three types of officials—special agents, targeters, and intelligence analysts. These officials come from either CBP or U.S. Immigration and Customs Enforcement (ICE). The team leader is a CBP officer or targeter who is assigned to serve as the immediate supervisor for all CSI team members and is responsible for coordinating with host government counterparts in the day-to-day operations. The team leader is also to prepare a weekly report on container targeting and inspection activity at the port. The targeters are team members responsible for targeting shipments and referring those shipments they determine are high-risk to host government officials for inspection. The targeter may also observe inspections of containers. The intelligence analyst is responsible for gathering information to support targeters in their efforts to target containers. In addition, the special agents are to coordinate all investigative activity resulting from CSI-related actions, as well as liaison with all appropriate U.S. embassy attachés.

CSI Process for Targeting and Inspecting Cargo Containers Overseas

Although the targeting of cargo at domestic ports is primarily dependent upon the ATS score, under CSI the targeting of cargo is largely dependent on CBP targeters' review of the ATS score in conjunction with reviews of bills of lading, additional information provided by host government officials, and, in at least one country, a unique set of targeting rules developed jointly by CBP and host government officials. As shown in figure 3, on the basis of the initial review, CBP officials are to either (1) categorize shipments as low-risk, in which case the container holding

the shipment is loaded onto the departing vessel without being inspected, or (2) conduct further research in order to properly characterize the risk level of the shipment.

Figure 3: CSI Process for Targeting and Inspecting Cargo Containers Overseas



Source: U.S. Customs and Border Protection.

Referrals of shipments to the host government for inspection are handled in one of three ways—shipments are inspected or inspection is either waived or denied. After receiving a referral for inspection from CSI teams, host customs officials are to review the bills of lading of the shipments and the reasons for the referrals to determine whether or not to inspect the shipments. Some host governments collect information on U.S.-bound shipments independent of CSI, which host officials also consider in decisions of whether to inspect the referred shipments. Finally, if the host government officials determine, on the basis of their review, that a shipment is not high-risk, they will deny inspection of the shipment. For any high-risk shipment for which an inspection is waived or denied, CSI teams are to place a domestic hold on the shipment, so that it will be inspected upon arrival at its U.S. destination. However, if CSI team members are adamant that a cargo container poses an imminent risk to the carrier or U.S. port of arrival but cannot otherwise convince the host officials to inspect the container, CSI team members are to contact and coordinate with the National Targeting Center to issue a do-not-load order for national security. According to CBP officials, this order advises the carrier that the specified container will not be permitted to be unloaded in the United States until a time when any associated imminent risk to the cargo container is neutralized. Once the risk is neutralized, the container is to be loaded back onto the carrier and placed on hold for a domestic examination. According to CBP officials, this type of do not load order has been implemented six times since the inception of CSI.

As in the domestic inspection process, there are, generally, two types of CSI inspections—nonintrusive inspections and physical inspections.[9] However, since CBP officials do not have the legal authority to inspect U.S.-bound containers in foreign ports, the host government customs officials are to conduct the inspections. According to CBP, in general, CBP officials are to observe the inspections and document inspection results. In addition, CBP officials, along with host government officials, may review the images produced by the X-ray or gamma-ray equipment to detect any anomalies that may indicate the presence of WMD.[10] Also in collaboration with host government officials, CBP officials are to review the output produced by radiation detection devices to assess whether

[9]Host government officials at one of the four CSI ports we visited conducted physical inspections of all containers referred to them by the CSI team.

[10]Host government officials at one of the four CSI ports we visited also used an explosive detection device during nonintrusive inspections.

radioactive or nuclear material is present. On the basis of the results of the nonintrusive inspection, such as if an anomaly is apparent in the image of the container, the host government and CBP officials must decide whether to conduct a physical examination of the container. Our limited observations at three ports confirmed that host nation officials allowed CSI team members to observe the inspection process. CBP and host government officials at the four CSI ports we visited indicated that if WMD or related contraband were found during a CSI inspection, the host government would be responsible for taking appropriate enforcement measures and disposing of the hazardous material.

While CBP Has Enhanced Its Ability to Target Containers Overseas, Limitations Remain

We identified both positive and negative factors that affect CBP's ability to target shipments at overseas seaports. According to CBP officials, the CSI program has produced factors that contribute to CBP's ability to target shipments at overseas seaports, including improved information sharing between the CSI teams and host government officials regarding U.S.-bound shipments and a heightened level of bilateral cooperation on and international awareness of the need for securing the global shipping system. However, we found several factors that may limit the program's effectiveness at some ports, including (1) staffing imbalances at CSI ports and (2) weaknesses in one source of data CBP relies upon to target shipments.

CSI Successes Have Enhanced CBP's Ability to Target Containers Overseas

One of the factors assisting with targeting of cargo is improved information sharing between U.S. and host customs officials. CBP has successfully negotiated agreements with several foreign governments to allow for the operation of CSI at their overseas seaports. Through September 11, 2004, CSI teams were able to target about 65 percent of the shipments coming through 25 CSI ports to determine whether they were at risk of containing WMD. This represented about 43 percent of all oceangoing cargo container traffic to the United States. As of January 2005, CBP had expanded the program to 34 operational ports, with plans to further expand the program to a total of 45 ports by the end of fiscal year 2005. According to CBP officials, the overseas presence of CBP officials has led to effective information sharing between the team and host government officials regarding targeting of U.S.-bound shipments. For example, CBP targeters at one of the ports we visited said that the presence of CBP officials at CSI ports fosters cooperation by host nation customs officials, such that more shipments characterized as high-risk and referred for inspection would be denied inspection by the host government if CBP officials were not present. According to CBP officials, information from host government officials on U.S.-bound shipments has

been beneficial to CBP's efforts to target shipments. They noted that the additional information provided by host governments can be utilized to address threats posed by U.S.-bound shipments. Additionally, CBP officials noted that the CSI teams can provide this information to NTC to incorporate into ATS to enhance CBP's targeting capabilities. During one of our port visits, host government officials noted that providing information to CSI teams allows CBP officials to make more informed decisions about which shipments are high-risk, reducing the number of shipments deemed high-risk and referred for inspection by the host government. Additionally, CBP and host government officials at this same port told us that host government information also results in additional inspections of U.S.-bound containers, beyond those referred by the CSI team. For example, they said that in 2003, this host government identified and inspected 30 high-risk U.S.-bound containers that were not identified as high-risk by the CSI team.

Another positive factor reported to us is the level of bilateral cooperation and international awareness regarding the need to secure global trade. With the discovery and seizure of shipments under CSI of automatic weapons, ammunition, and other falsely identified contraband, CBP noted that many customs services around the world without strong law enforcement capabilities are currently seeking additional legal authority to strengthen their ability to fight terrorism. For example, CBP noted that in June 2002, the World Customs Organization (WCO) passed a resolution to enable ports in all of its member nations to begin to develop outbound targeting programs consistent with the CSI model. In addition, in April 2004 the European Union and the Department of Homeland Security signed an agreement that calls for intensifying and broadening the agreement on customs cooperation and mutual assistance in customs matters, to include cooperation on container security and related matters. For example, the measures adopted in the agreement include the creation of an information exchange network, an agreement on minimum requirements applicable for European ports that wish to participate in CSI, and identification of best practices concerning security controls of international trade.

CBP Staffing Imbalances Prevent Targeting of All Containers from CSI Ports

One factor negatively affecting CBP's ability to target containers is staffing imbalances across ports and shortages at some ports. Although CBP's goal is to target all U.S.-bound containers at CSI ports before they depart for the United States, it has not been able to place enough staff at some CSI ports to do so. CBP has developed a CSI staffing model to determine the staff needed to target containers. However, at some CSI ports CBP has been unable to staff the CSI teams at the levels called for in the CSI

staffing model. In commenting on a draft of this report, DHS noted that the 35 percent of U.S.-bound shipments that were not targeted by CSI teams were deemed low-risk by ATS and thus required no further review at CSI ports. However, our discussions with CSI teams at two of the four ports we visited indicated that those teams did not prioritize shipments for targeting based on ATS score but instead prioritized shipments by departure time. As a result, there is no assurance that all high-risk shipments are targeted at CSI ports.

CBP has been unable to staff the CSI teams at the levels called for in the CSI staffing model because of diplomatic and practical considerations. CBP officials told us it is unrealistic to expect that CBP can place the number of targeters indicated by its staffing model needed to review all shipments at every CSI port. In terms of diplomatic considerations, the host government may limit the overall number of U.S. government employees to be stationed in the country and may restrict the size of the CSI team. In terms of practical considerations, the host governments may not have enough workspace available for CSI staff and may thus restrict the size of the CSI team. The U.S. Department of State would also have to agree to the size of the CSI teams, a decision that has to be balanced with the mission priorities of the embassy, the programmatic and administrative costs associated with increases in staffing, and security issues related to the number of Americans posted overseas. According to the State Department, the average cost of putting an American position overseas will be approximately $430,000.[11]

One of the features of the CSI staffing model that may contribute to the staffing imbalance is its reliance on placing staff overseas at CSI ports. It does not consider whether some of the targeting functions could be performed in the United States. For example, the model does not consider what minimum number of targeters need to be physically located at CSI ports to carry out duties that require an overseas presence (such as coordinating with host government officials) as opposed to other duties that could be performed in the United States (such as reviewing manifests and databases). As we noted in our 2002 report on a staffing framework for use at U.S. embassies, federal agencies should consider options that improve operational efficiency and effectiveness and that minimize

[11]U.S. Office of Management and Budget, Department of State and International Assistance Programs, *Budget of the United States Government, Fiscal Year 2006* (Washington, D.C.: February 2005).

security risks, such as assessing which functions can occur in the United States, as part of their framework for determining the right number of staff to be placed overseas.[12]

CBP has acknowledged that it cannot fully implement the CSI staffing model and has supplemented staff at the CSI ports with domestic targeters at NTC. According to CBP officials, CSI teams may contact these NTC targeters and request that they help target specific shipments that CSI teams at the ports are unable to target. The NTC targeters, after targeting the shipments, are to notify the relevant CSI team with the results of their targeting, including whether the shipments are high-risk and should be referred to the host government for inspection. Although the NTC targeters are available to provide assistance to CSI teams 24 hours a day, 7 days a week, CBP officials noted that even with the addition of these targeters, the bureau has been unable to target every U.S.-bound shipment before it departed a CSI port.

The use of domestic targeters demonstrates that CBP does not have to rely exclusively on overseas targeters as called for in its staffing model. Our observations at four CSI ports indicated that having CSI staff work directly with host nation customs officials was beneficial to both the targeting and the inspection processes. However, we also noted that the the targeters' work focused on targeting ATS findings, as well as consulting various automated databases, and did not include much interaction with host government officials. For example, at two of the ports we visited CBP officials told us that typically only one or two CSI team members dealt directly with host customs officials. In addition, while CBP officials could not provide us with port-specific or average costs of the CSI port teams, they stated that it was more expensive to post staff overseas than in the United States.

One Source of Targeting Data Has Limitations

Another factor that negatively affects CBP's ability to target shipments is the existence of limitations in one data source used. For CSI, CBP relies on manifest information to assess the risk level of U.S.-bound shipments.[13]

[12]GAO, *Overseas Presence: Framework for Assessing Embassy Staff Levels Can Support Rightsizing Initiatives*, GAO-02-780 (Washington, D.C.: July 2002).

[13]According to CBP officials, importers typically do not submit entry-level data to CBP at the same time that manifest data are submitted. As a result, only limited entry-level data are available at the time of review.

As we previously reported, terrorism experts, trade representatives, and CBP officials indicated that manifest data may contain unreliable information and are sometimes incomplete.[14] We reported that manifests are produced by second-hand parties (ocean carriers), not the importers or exporters who have the most contact with and knowledge of the cargo. In addition, manifests have historically been used to disguise detailed information about containers' contents, to prevent theft during transport of the cargo. This is particularly applicable to high-value products, such as electronics and apparel. In the same previous report, we also noted that manifest data can be amended up to 60 days after oceangoing vessels arrive at U.S. seaports, further limiting the use of manifest data for determining a definitive risk level before cargo arrives.[15] CBP officials at CSI ports we visited indicated that despite the requirement that carriers submit accurate and complete manifests to CBP 24 hours prior to the cargo being loaded on the U.S.-bound vessel, some manifest data in ATS remain vague or incomplete. For example, a CBP official at one CSI port we visited said that in some cases the name of the freight forwarder was used in place of the actual names of the importer and consignee. Although CBP officials told us that the quality of the manifest data has improved, there is no method to routinely verify whether the manifest data accurately reflect the contents within the cargo container. CBP officials told us that to try to address the shortcomings of manifests, CSI teams consult other data to obtain information on shipments. As mentioned earlier, entry-level data are used.

Some Containers Not Inspected for a Variety of Reasons

Since the implementation of CSI through September 11, 2004, 28 percent (4,013) of containers referred to host government officials for inspection were not inspected, generally because of host government information that suggested the containers were not high-risk or operational limitations that prevented the containers from being inspected before they left the port. In 1 percent of these cases, host government officials denied inspections, generally because inspection requests were based on factors not related to security threats, such as drug smuggling. Containers designated as high-risk by CSI teams that are not inspected overseas are supposed to be referred for inspection upon arrival at the U.S. destination

[14]GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: February 20, 2004).

[15]GAO-04-557T. The regulations governing submission of amended manifest data are located in 19 CFR 4.12.

port. CBP officials noted that between July 2004 and September 2004, about 93 percent of shipments referred for domestic inspection were inspected at a U.S. port. CBP officials explained that some shipments designated as high-risk by CSI teams were not inspected domestically because inspectors at U.S. ports received additional information or entry information that lowered the risk characterization of the shipments or because the shipments remained aboard the carrier and were never offloaded at a U.S. port. For the 72 percent (10,343) of containers referred to host government officials for inspection that were inspected overseas, CBP officials told us there were some anomalies that led to law enforcement actions but that no WMD were discovered. However, considering that the inspection equipment used at CSI ports varies in detection capability and that there are no minimum requirements for the detection capability of equipment used for CSI, CBP has no absolute assurance that inspections conducted under CSI are effective at detecting and identifying WMD.

Some Containers Not Inspected Overseas because of Host Government Information

Some of the containers referred for inspection were not inspected because of additional information obtained by host government officials that lowered the risk characterization of the container. An important aspect of CSI is the information host government officials can provide in determining whether a U.S.-bound container is at high risk of containing WMD and should be inspected. For example, at one CSI port we visited, the host customs official told us that although CBP officials referred a shipment for inspection because the area from which the shipment originated had known terrorist activity, the host government's customs officials had a thorough working history with the importer and believed the shipment did not pose a threat. On the basis of this information, the CSI team and the host nation customs officials agreed that the shipment did not pose a threat and that inspection was not necessary.

Some Containers Not Inspected Overseas because of Operational Limitations

Some containers were not inspected at CSI ports because of operational limitations that were generally beyond the control of CBP. For example, since the program's inception through September 11, 2004, some referred containers were not inspected at CSI ports because the containers had already been loaded on departing vessels. CBP officials and host government customs officials explained that a container may already be loaded on a vessel prior to its being referred for inspection because the amount of time the container actually stays in the port—dwell time—may be brief. CSI teams are not always able to target such containers and refer them for inspection before they are loaded. According to CBP and host

government officials with whom we met, terminal operators intentionally schedule the arrival and departure of containers in order to minimize dwell time. However, CSI teams may not always know when containers are due for departure. Host government customs officials at one of the ports we visited said that until recently, the CSI team did not have access to the port schedules for U.S.-bound containers; therefore, team members could not prioritize the order in which they reviewed bills of lading for U.S.-bound shipments based on container dwell time. However, as of July 2004, the CSI team at this port gained access to port schedule information and now prioritizes its review of bills of lading based on container departure time. Host government officials noted that this practice decreases the number of containers waived for inspection.

Host Nations Deny Inspections for Some Containers Referred by CSI Teams

In addition to operational limitations that prevent referred containers from being inspected at CSI ports, host government officials have denied inspection for about 1 percent of the containers referred to them by CBP officials. According to CBP officials, the majority of these denials occurred early in the program's operation as both CSI teams and host government officials implemented the program. For example, host government officials at one CSI port we visited indicated that some of these denials were for inspection requests based on factors not related to security threats, such as drug smuggling. They told us their rationale in denying these requests was that CBP could inspect these containers in the United States, and identifying customs violations was not the purpose of CSI. At another port we visited, CSI team officials told us that host customs officials initially denied inspections of shipments referred solely because of the shipment's ATS score, preferring to instead have referrals that were further researched by the CSI team to help ensure that shipments were truly high-risk. As noted earlier, if the CSI team members are adamant that a cargo container poses an imminent risk to the conveyance or the U.S. port of arrival, they can coordinate with the National Targeting Center to issue a do-not-load order to prevent the container from being placed on the ship.

Containers Not Inspected Overseas Can Be Inspected on U.S. Arrival

Containers with high-risk shipments that are not inspected overseas are supposed to be referred for inspection upon arrival at the U.S. destination port. Effective November 21, 2003, CSI team members were required to place domestic exam holds on high-risk containers that had not been inspected overseas. That is, the CSI team is supposed to request a domestic inspection for all containers for which an inspection was waived or denied by marking, in ATS, the container for a domestic hold and notifying the director of the U.S.-destination port. The CSI team is also

supposed to request domestic exams for shipments that were inspected overseas but not to the satisfaction of the CSI team, such as if there was a disagreement over the interpretation of the X-ray image produced during the nonintrusive inspection or if the host nation was not willing to perform a physical exam after an anomaly was detected. However, not all shipments referred for a domestic inspection by CSI teams are inspected. Although CBP has not systematically tracked since the program's inception whether containers placed on domestic hold are examined, according to CBP, it began tracking this information in July 2004. CBP officials told us that between July 2004 and September 2004, 93 percent of the shipments placed on CSI for domestic exam hold were actually inspected at a U.S. port. CBP explained that U.S. port officials did not inspect about 2 percent of the shipments placed on domestic exam hold during this time period because the shipments were either remaining on board at the U.S. port or additional intelligence information convinced them that the shipment no longer needed to be characterized as high-risk. For the remaining 5 percent of shipments that were not inspected domestically, CBP officials told us the bureau cannot confirm what action was taken on these shipments because of data input errors by domestic inspectors. CBP officials also noted that they were unable to confirm whether any shipments placed on domestic exam hold prior to July 2004 were actually inspected upon arrival in the United States because of these same data input errors.

In the Absence of Minimum Technical Requirements, Inspection Equipment Capabilities Vary

As of September 11, 2004, host governments had inspected 72 percent (10,343) of all containers referred to them by CSI teams since the inception of the program. These containers were inspected using nonintrusive inspections and physical examinations. According to CBP and host government officials, variation in the extent of physical examinations depends on anomalies detected during the nonintrusive inspection. CBP officials also told us that no WMD have been discovered under CSI.

There are two different types of radiation detection devices used at CSI ports to inspect cargo containers—radiation isotope identifier devices (RIID) and radiation portal monitors (RPM)—each with different detection and identification capabilities. While both devices can detect the presence of radioactive material, only the RIID can determine whether or not the type of radiation emitted by the material actually poses a threat or whether it is a normal emission of radiation, such as that found in ceramic tile. In addition, there is another type of radiation detection device used at CSI ports to help ensure the safety of CSI team members—personal

radiation detectors (PRD). According to radiation detection experts, PRDs are personal safety devices to protect against radiation exposure, they are not adequate as search instruments. A scientist at the Department of Energy Los Alamos National Laboratory who was involved in the testing of radiation detection equipment said that PRDs have a limited range and are not designed to detect weapons-usable nuclear material.

There are also various types of X-ray and gamma-ray imaging machines used at CSI ports to inspect cargo containers, and their detection and identification capabilities may vary. According to CBP, there are various brands of imaging machines used to conduct nonintrusive inspections at CSI ports. These brands of machines differ in their penetration capabilities, scan speed, and several other factors. Despite this variability in detection and inspection capability, CBP officials told us that the inspection equipment used at all CSI ports had inspection capabilities at least as good as the nonintrusive inspection equipment used by CBP at domestic ports. CBP officials told us that prior to establishing CSI at a foreign port, CBP officials conducted on-site assessments of the nonintrusive inspection equipment used at the port. More recently, CBP conducted an assessment of the capabilities of the equipment in use at each CSI port against the capabilities of one brand of equipment. This assessment indicated that with the exception of equipment used in one country, all equipment had capabilities that met or exceeded those of this brand of equipment. In addition, technologies to detect other WMD have limitations. According to CBP officials, the bureau has not established minimum technical requirements for the nonintrusive inspection equipment or radiation detection equipment that can be used as part of CSI because of sovereignty issues, as well as restrictions that prevent CBP from endorsing a particular brand of equipment. Although CBP cannot endorse a particular brand of equipment, the bureau could still establish general technical capability requirements for any equipment used under CSI similar to other general requirements CBP has for the program, such as the country committing to establishing an automated risk management system. Because the CSI inspection could be the only inspection of a container before it enters the interior of the United States, it is important that the nonintrusive inspection and radiation detection equipment used as part of CSI meets minimum technical requirements to provide some level of assurance of the likelihood that the equipment could detect the presence of WMD.

CBP Has Made Progress Developing a Strategic Plan and Performance Measures for CSI, but Further Refinements Are Needed

Although CBP has made some improvements in the management of CSI, we found that further refinements to the bureau's management tools are needed to help achieve program goals. In July 2003, we recommended that CBP develop a strategic plan and performance measures, including outcome-oriented measures, for CSI. In February 2004, CBP finalized a strategic plan for CSI containing three of the six key elements identified by the Government Performance and Results Act of 1993 (GPRA) for an agency strategic plan: a mission statement, objectives, and implementation strategies. CBP officials told us the bureau plans to incorporate the remaining three elements into the CSI strategic plan, specifying how performance goals are related to general goals of the program, identifying key external factors that could affect program goals, and describing how the program will be evaluated. CBP has also made progress in the development of outcome-oriented performance measures for some objectives, particularly for the objective of increasing information sharing and collaboration among CSI and host country personnel. However, further refinements are needed to assess the effectiveness of the other program objectives, including CSI targeting and inspection activities.

CBP Completed a Strategic Plan for CSI, but Three Key Elements Are Still under Development

In July 2003, we recommended that CBP develop a strategic plan for CSI. CBP developed a strategic plan in February 2004. According to GPRA, executive agency strategic plans should include

- a comprehensive mission statement,
- general goals and objectives,
- a description of how the general goals and objectives are to be achieved,
- a description of how performance goals and measures are related to the general goals and objectives of the program,
- an identification of key factors external to the agency and beyond its control that could affect the achievement of general goals and objectives, and
- a description of the program evaluations.

These six key elements are required for executive agency strategic plans and thus serve as a good baseline to measure other long-term planning efforts. In addition, we have found that high-quality plans include

strategies to mitigate the effects of external factors, although such strategies are not a legislative requirement.[16]

CSI's strategic plan includes three of these key elements:

- a mission statement: "to prevent and deter terrorist use of maritime containers while facilitating movement of legitimate trade";
- objectives, including (a) pushing the United States' zone of security beyond its physical borders to deter and combat the threat of terrorism; (b) targeting shipments for potential terrorists and terrorist weapons, through advanced and enhanced information and intelligence collection and analysis, and preventing those shipments from entering the United States; (c) enhancing homeland and border security while facilitating growth and economic development within the international trade community; and (d) utilizing available technologies to leverage resources and to conduct examinations of all high-risk containers (another objective cited by CBP officials, although not included in the CSI strategic plan, is to raise the level of bilateral cooperation and international awareness regarding the need to secure global trade); and
- various descriptions of how general goals and objectives are to be achieved.

However, CBP has not yet incorporated the other three key elements into its strategic plan. For example, the CSI strategic plan does not include a description of how performance goals and measures are related to program objectives. At the time the strategic plan was developed, CBP lacked performance goals and measures. We discuss performance measures in more detail in the next section.

In addition, the CSI strategic plan does not identify external factors beyond the control of CBP that could affect the achievement of program objectives. Such external factors could include economic, demographic, social, technological, or environmental factors. Two external factors that could be addressed in the CSI strategic plan are the extent to which host governments can provide additional information to contribute to the targeting process and the various operational limitations that prevent all high-risk containers from being inspected overseas.

[16]GAO, *Results-Oriented Government: GPRA Has Established a Solid Foundation for Achieving Greater Results*, GAO-04-38 (Washington, D.C.: March 10, 2004).

In addition, the CSI strategic plan does not include a description of program evaluations. Although evaluations are not described in the CSI strategic plan, CBP conducts periodic evaluations of CSI ports in order to determine areas in which implementation of CSI can be improved and to determine whether CSI should continue to operate at that port. However, these evaluations do not employ a systematic methodology or identify the basis on which program success is determined. GPRA defines a program evaluation as an objective and formal assessment of the implementation, results, impact, or effects of a program or policy. Program evaluations are used to ensure the validity and reasonableness of program goals and strategies, as well as identify factors likely to affect program performance. Specifically, CBP has not identified and planned which CSI elements will be assessed at each port; rather, assessment topics are generated ad hoc. In addition, assessment topics differ over time, preventing CBP from determining the extent to which CSI teams addressed issues raised in previous evaluations. For example, in its July 2003 evaluation of one CSI port, CBP's Office of International Affairs identified the following problems: (1) lack of information available to the intelligence research specialist, (2) the need to make better information available to CSI team members, and (3) the lack of follow-through on shipments through CSI ports that were referred for domestic exam. However, none of these issues was discussed in the Office of International Affairs' next evaluation of this port in December 2003. Similarly, the assessment topics for CSI port evaluations also differ across ports, making it difficult to make comparisons across ports.

In February 2005, CBP officials told us that CBP is revising the CSI strategic plan to address the elements we raise in this report. While it appears that the bureau's initial efforts in this area meet the intent of our prior recommendation to develop a strategic plan for CSI, we cannot determine the effectiveness of further revisions to the plan without first reviewing and evaluating them. We will continue to monitor CBP's efforts in this area.

CBP Has Developed Outcome-Oriented Performance Measures for Some Program Objectives

In July 2003, we recommended that CBP expand efforts already initiated to develop performance measures for CSI that include outcome-oriented indicators. Until recently, CBP based the performance of CSI on program outputs such as (1) the number and percentage of bills of lading reviewed, further researched, referred for inspection, and actually inspected, and (2) the number of countries and ports participating in CSI.

As of January 2005, CBP had developed 11 performance indicators for CSI, 2 of which it identified as outcome-oriented: (1) the number of foreign mitigated examinations and (2) the percentage of worldwide U.S.-destined containers processed through CSI ports.[17] As indicated in table 2, both outcome indicators are used to assess CBP's progress in meeting its objective of increasing information sharing and collaboration among CBP officials and host country personnel.

[17]In addition to the outcome measures listed in table 4, CBP also developed what the bureau calls information measures to gauge CBP's progress in increasing information sharing and collaboration among CSI and host country personnel. See appendix II for a description of these and other CSI performance measures.

Table 2: CSI Outcome-Oriented Performance Measures

Measure	Scope	FY 2004 baseline	Cumulative FY 2005 target	Long-term program goal
Number of foreign mitigated examinations, by category	The measure will be the number of examinations waived for a variety of reasons.	2,416 (cumulative)	Increase over baseline; track by categories	Increase information sharing and collaboration among CSI and host country personnel so that the number of foreign mitigated container exams is increased and legitimate trade is facilitated through the port
Percentage of worldwide U.S.-destined containers processed through CSI ports	This measure will utilize the annual volume of U.S.-destined containers processed through all CSI ports prior to lading and divide it by the annual worldwide number of U.S.-destined containers.	48%	68%	Increase information sharing and collaboration among CSI and host country personnel in order to prevent terrorist weapons from entering the country

Source: CBP.

However, the way in which one of these indicators is measured needs refinement. The measure for the number of foreign mitigated examinations is the number of shipments referred to host governments that were not, for a variety of reasons, inspected overseas. Specifically, according to CBP, an increase in the number of examinations waived or denied suggests an increase in the number of unnecessary examinations that were prevented. However, the number of examinations waived or denied by host nations are not appropriate measures for the prevention of unnecessary exams. A shipment is inspected unnecessarily if, when provided with additional information on the shipment, the CSI team and the host nation would have agreed that the shipment was not high-risk and, therefore, the inspection should not have taken place. However, if an inspection is waived because of operational limitations, the implication may not be that the CSI team thinks the inspection is unnecessary. To the contrary, the CSI team and host government may agree that the shipment should be inspected. Similarly, a host nation denial of an inspection does not imply that the CSI team believes the inspection is unnecessary. Conversely, when a referral for inspection is categorized as denied, by definition, the CSI team believes the shipment should be inspected, but the host government refuses to conduct the inspection. In response to our review, CBP officials acknowledged that its inclusion of waivers because of operational limitations or denials of inspections in this measure was inappropriate.

CBP noted that each of the performance measures for assessing information sharing and collaboration with host nations will be pilot-tested at numerous CSI ports to assess their feasibility, utility, relevancy, and the likelihood that they will produce information that is actionable. According to CBP, the measures may be revised based on the evaluation of the pilot to improve their effectiveness in assessing program performance and outcomes.

According to Office of Management and Budget (OMB) and CBP officials, developing outcome-oriented performance measures that measure the effectiveness of programs that aim to deter or prevent specific behaviors is challenging. For example, one of CSI's objectives is to deter terrorists' use of oceangoing cargo containers. However, according to host government officials at one port we visited and CBP officials, it is difficult to develop a meaningful measure for the extent to which implementation of CSI has discouraged terrorists from using oceangoing cargo containers to smuggle WMD into the United States. In January 2005, CBP developed a performance indicator to measure CSI's progress in preventing terrorists' use of oceangoing cargo containers that measures the amount of terrorist contraband, illegal drugs, and other illegal activity found during CSI inspections. However, this indicator may not be a meaningful measure of deterrence of terrorist activity, since the inclusion of narcotics is not relevant to the program's objectives, and according to CBP, no terrorist weapons or weapons material have been detected prior to or during the implementation of CSI.

According to OMB, when agencies face difficulty in developing outcome-based performance measures, they are encouraged to develop proxy measures. Proxy measures are used to assess the effectiveness of program functions, such as the targeting and inspection processes of CSI, rather than directly assess the effectiveness of the program. For example, CBP could develop a proxy measure associated with targeting and inspection, such as the percentage of containers randomly inspected domestically that was not characterized by CBP officials as high-risk that actually contained WMD. CBP could also use random inspections to measure if containers from CSI ports that were not identified as high-risk actually contained WMD and, therefore, should have initially been identified as high-risk. According to terrorism experts and representatives of the international trade community, random inspections could be an effective practice to supplement and test CBP's targeting and inspection processes.

Terrorism experts and shipping industry representatives also suggest that staging covert, simulated terrorist events could test the effectiveness of

both the targeting and inspection processes of CSI. Simulated events could include smuggling fake WMD into the United States using an oceangoing cargo container. Such events could help determine whether the targeting procedures led to the identification of the container as high-risk and whether any subsequent inspection activities actually detected the fake WMD. CBP could, therefore, develop proxy measures associated with this activity for CSI, such as the percentage of staged containers that were identified as high-risk and the percentage of staged containers for which the fake WMD was detected during the inspection process. In response to our prior work on container security, CBP officials agreed with our recommendation that containers be subject to such tests.

CSI lacks performance goals and measures for its objective of enhancing homeland and border security while facilitating growth and economic development within the international trade community. Regarding the enhancement of homeland and border security, there are no performance goals for CSI. According to host government officials at CSI ports we visited and shipping industry representatives with whom we met, CSI has resulted in increased international awareness of supply chain security. Officials from the World Customs Organization predicted that as more countries partner with CBP through CSI, there will be increased consistency in the way in which the supply chain and ports are secured worldwide. One WCO official also stated that CBP's efforts through initiatives such as CSI provide guidance for developing countries on how to improve their supply chain security efforts. While these testimonials help identify some benefits of CSI, CBP does not have performance indicators and goals to actually measure the extent to which the program has resulted in enhanced homeland and border security.

Regarding facilitating economic growth, there are also no performance measures for CSI. According to host government officials with whom we met at one CSI port, they are willing to participate in CSI as long as the program does not disrupt the flow of trade. An example of such a disruption would be the delayed departure of a vessel because of a CSI inspection or the instruction not to load a container on a departing vessel because of a CSI inspection. Discussions with CBP and host government officials and representatives of the shipping industry indicate that CBP has been successful in not disrupting the flow of trade through CSI. However, CBP has not developed associated performance goals and measures to demonstrate its reported success in achieving this objective. In commenting on a draft of this report, DHS noted that CBP is continuing to refine existing performance measures and develop new performance measures for its program goals. For example, CBP was developing a cost

efficiency measure to measure the cost of work at a port and to contribute to staffing decisions. CBP believes that its continued revisions to the CSI strategic plan have also allowed CSI staff to refine performance measures and the bureau's data collection methodology.

Conclusions

CBP has made progress in its implementation of CSI, but the program could be further improved by taking steps to help ensure its effectiveness in preventing WMD from entering the United States via cargo containers. First, CBP's inability to staff all CSI ports to the level suggested by its staffing model and the model's assumption that all staff should be located at the CSI ports have limited the program's ability to target potentially high-risk shipments at some foreign seaports before they depart for the United States. This problem may be exacerbated as CBP continues to expand CSI to additional overseas seaports. Second, without minimum technical requirements for the nonintrusive inspection equipment used as part of CSI, CBP has limited assurance that the equipment in use can successfully detect all WMD. While we recognize that establishing such requirements may be a difficult issue to address, it is important that CBP establish them because the CSI inspection may be the only inspection of some containers before they enter the interior of the United States. Third, CBP has developed a strategic plan for the CSI program and indicated that it will refine the plan to include key elements described in GPRA. Although we are not making a recommendation related to its strategic plan, given the importance of having an effective strategic plan for the program, we will continue to monitor the bureau's progress in refining the plan. Finally, while CSI has apparently resulted in some benefits, such as cooperation with foreign governments and enhanced international awareness of container security, CBP has not developed outcome-based performance measures or proxy measures for all of its program objectives. Without outcome-based performance measures on which to base program evaluations, CBP will have difficulties assessing the effectiveness of CSI as a homeland security program.

Recommendations for Executive Action

To help ensure that the objectives of CSI are achieved, we recommend that the Secretary of the Department of Homeland Security direct the Commissioner of U.S. Customs and Border Protection take the following three actions:

- revise the CSI staffing model to consider (1) what functions need to be performed at CSI ports and what functions can be performed in the United States, (2) the optimum levels of staff needed at CSI ports to maximize the benefits of targeting and inspection activities in

conjunction with host nation customs officials, and (3) the cost of locating targeters overseas at CSI ports instead of in the United States;

- establish minimum technical requirements for the capabilities of nonintrusive inspection equipment at CSI ports, to include imaging and radiation detection devices, that help ensure that all equipment used can detect WMD, while considering the need not to endorse certain companies and sovereignty issues with participating countries;
- develop performance measures that include outcome-based measures and performance targets (or proxies as appropriate) to track the program's progress in meeting all of its objectives.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of DHS and the Department of State for comment. We received comments from the DHS Acting Director, Departmental Liaison, that are reprinted in appendix III. DHS generally agreed with our recommendations and outlined actions CBP either had taken or was planning to take to implement them. The Department of State had no comments.

CBP agreed with our recommendation on CSI's staffing model and said that modifications to the model would allow for program objectives to be achieved in a cost-effective manner. Specifically, CBP said that it would evaluate the minimum level of staff needed at CSI ports to maintain an ongoing dialogue with host nation officials, as well as assess the staffing levels needed domestically to support CSI activities. If properly implemented, these actions should address the intent of this recommendation.

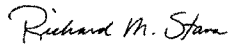
In addressing our recommendation to establish minimum technical requirements for the capabilities of the nonintrusive inspection equipment used at CSI ports, CBP agreed to evaluate the feasibility of making such requirements for the imaging and radiation detection devices in use at CSI ports but did not commit to implement our recommendation. CBP noted that because host governments purchase the equipment for use at CSI ports, a legal issue may exist regarding CBP's ability to impose such requirements. CBP noted it would also seek comment and advice from other U.S. government agencies that would be affected by such a decision. Although CBP cannot endorse a particular brand of equipment, the bureau could still establish general technical capability requirements for any equipment used under CSI similar to other general requirements CBP has for the program, such as the country committing to establishing an

automated risk management system. Because the CSI inspection could be the only inspection of a container before it enters the interior of the United States, it is important that the nonintrusive inspection and radiation detection equipment used as part of CSI meet minimum technical requirements to provide some level of assurance of the likelihood that the equipment could detect the presence of WMD.

CBP agreed with our recommendation on developing performance measures, noting that it would continue to refine, evaluate, and implement any and all performance measures needed to track the progress in meeting all of CSI's objectives. CBP noted that this would be an ongoing activity. If properly implemented, these plans should help address the intent of this recommendation.

DHS also offered technical comments and clarifications, which we have considered and incorporated where appropriate.

If you or your staffs have any questions about this report, please contact me at (202) 512-8777 or at stanar@gao.gov. Key contributors to this report are listed in appendix IV. This report will also be available at no charge on the GAO Web site at http://www.gao.gov.



Richard M. Stana
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

We addressed the following issues regarding the U.S. Customs and Border Protection's (CBP) Container Security Initiative (CSI):

- What factors affect CBP's ability to target high-risk shipments at overseas seaports?
- Under CSI, to what extent have high-risk containers been inspected overseas prior to their arrival at U.S. destinations?
- To what extent has CBP developed strategies and related management tools for achieving the program's goals?

Scope and Methodology

To address our first issue—what factors affect CBP's ability to target shipments at overseas seaports—we first reviewed relevant GAO reports on CBP's Automated Targeting System (ATS) and CSI. We then met with CBP headquarters officials to hold discussions and review documents related to CSI's overall targeting strategy, criteria for identifying high-risk containers, efforts to evaluate the program, efforts to refine targeting, training provided to CSI targeters, and the criteria for staffing at CSI ports. We also visited the National Targeting Center, which serves as CBP's central targeting facility related to terrorism. At this facility, we met with cognizant officials and discussed ATS categorization of containers by risk level, how cargo containers' scores are transmitted to targeters at CSI ports, the training provided to the ATS targeters, the types of information and intelligence utilized by targeters, and recent and planned refinements to ATS. We also met with officials from the European Commission and the World Customs Organization (WCO) in Brussels, Belgium, and discussed how the CSI program has been implemented and its impact on container security.

Also related to this first issue, we visited four overseas CSI ports. We selected these ports on the basis of the volume of containers shipped to the United States, geographic dispersion, and time the CSI team was in operation. At these ports, we met with the CSI teams to discuss and review documents related to the overall targeting process, the types of information used in the targeting process, efforts to evaluate the targeting process, the impact other CBP initiatives may have had on the targeting process, and requests for information to host governments. We also observed operations at each of the ports, including targeters reviewing manifest information.

To address our second issue—to what extent have high-risk containers been inspected overseas prior to their arrival at U.S. destinations—we met with officials from CBP headquarters and CSI port teams to hold discussions and review documents related to the overall inspection process, types of inspections, inspection equipment used, statistics on inspections conducted at CSI ports, and levels of cooperation with host governments. At the four ports we visited, we also met with foreign government customs officials to discuss the role of the CSI teams in the inspection process, the criteria they use in deciding whether to inspect a container that was referred for inspection by the CSI team, the criteria they use in deciding the type of inspection to be conducted, the procedures they use to safeguard containers once inspected, and the types of inspection equipment they used.

To address our third issue—to what extent has CBP developed clearly formulated and documented strategies for achieving the program's goals—we reviewed GAO reports examining management factors that were necessary components for the successful management of cabinet departments, agencies, and, by extension, individual programs. Specifically, we focused our review on two management factors—the development of performance measures and strategic planning—because of their general importance in the literature. We reviewed Office of Management and Budget (OMB) and Government Performance and Results Act of 1993 (GPRA) guidance on performance measures and goals to assess the extent CBP has incorporated them into the CSI program. We also discussed CSI strategies for achieving program goals with officials from CBP headquarters, CSI teams, and host governments. We also obtained and reviewed CBP evaluations of CSI port teams to assess the methodology used to conduct evaluations.

We conducted our work from February 2004 through February 2005 in accordance with generally accepted government auditing standards.

Data Reliability

To assess the reliability of CBP's data on the number of shipments and containers subject to targeting and inspection under CSI, we (1) obtained source data on targeting and inspection activity for two 1-week periods from CSI teams at two ports, (2) compared the source data with the data generated by CBP's Automated Targeting System (ATS) for the same 2-week period, (3) discussed discrepancies between the source data and ATS data with CBP officials at these ports, and (4) obtained CBP headquarters' responses to our questionnaire regarding the reliability of ATS and the data that are produced by the system. Although our initial

reliability testing indicated that there were some inconsistencies between the source data and the data generated by ATS, generally because of human input error, we were able to work with CSI team officials to resolve most of the discrepancies. In addition, the differences between the source data and ATS data were so small that the results of our analysis, at least for this 2-week period, would have remained the same regardless of which data we used. Therefore, we determined that the CSI targeting and inspection data generated by ATS are sufficiently reliable for use in supporting our findings regarding the extent to which high-risk containerized shipments are identified and inspected prior to arrival at U.S. destinations.

Appendix II: CSI Performance Measures, as of January 2005

Measure	Scope	FY 2004 baseline	Cumulative FY 2005 target	Long-term program goal
Outcome measures				
Number of foreign mitigated examinations, by category	The measure will be the number of examinations waived because of a variety of reasons.	2,416 examinations (cumulative)	Increase over baseline; track by categories	Increase information sharing and collaboration among CSI and host country personnel so that the number of foreign mitigated container exams is increased and legitimate trade is facilitated through the port
Percentage of worldwide U.S.-destined containers processed through CSI ports	This measure will utilize the annual volume of U.S.-destined containers processed through all CSI ports prior to lading and divide it by the annual worldwide number of U.S.-destined containers.	48%	68%	Increase information sharing and collaboration among CSI and host country personnel in order to prevent terrorist weapons from entering the country
Information measures				
Number of intelligence reports based on CSI foreign sources	This measure will track the number of memorandums of information received (MOIR), which are narratives of intelligence gathered from CSI foreign sources.	17 cases	Increase over baseline	Increase information sharing and collaboration among CSI and host country personnel in order to prevent terrorist weapons from entering the country
Number of operational CSI ports	This measure identifies the total number of ports where CSI has been implemented.	30 ports	45 ports	Increase information sharing and collaboration among CSI and host country personnel in order to prevent terrorist weapons from entering the country

Measure	Scope	FY 2004 baseline	Cumulative FY 2005 target	Long-term program goal
Number of positive findings, by category	This measure includes identifying the number and type of "positive findings" documented because of CSI participation. Positive findings occur when examinations performed on containers yield a positive result such as implements of terror, narcotics, forced labor, uninvoiced or unmanifested good, restricted merchandise, hazardous materials, or other results. Note that the CSI goal is to find implements of terror; other categories are peripheral benefits.	Baseline to be established	Target to be established	Prevent terrorists, means of terrorism, illegal drugs, and other illegal activity
Number of investigative cases initiated because of CSI intelligence	This measure tracks the number of investigative cases opened either in the United States or at a foreign location because of intelligence gathered by CSI staff at foreign ports.	20 cases	10 percent increase over the baseline—22 cases	Increase information sharing and collaboration among CSI and host country personnel in order to prevent terrorist weapons from entering the country
Efficiency measure				
Average cost per CSI port to achieve operational status	The average cost per CSI port includes site assessments and certifications, telecom circuit installation, local area network (LAN) and office equipment, commercial off-the-shelf software, office furniture, radiation isotope identification devices (RIID), purchase of automobiles, initial lease and utilities costs, and initial shipping costs.	$395,000	$403,000	Increase information sharing and collaboration among CSI and host country personnel so that the number of foreign mitigated container exams is increased and legitimate trade is facilitated through the port

Measure	Scope	FY 2004 baseline	Cumulative FY 2005 target	Long-term program goal
Implementation measures				
Cumulative number of countries with signed declarations of principles	This measure records the number of declarations of principles signed with countries where CSI ports are planned.	20 countries	30 countries	Not applicable
Cumulative number of CSI ports with completed capacity assessments	These data will come from the number of completed pre-operational assessments that are on file for CSI ports	43 ports	51 ports	Not applicable
Number of CSI ports with completed infrastructures	This measure records the engineering statements of work that have been completed for candidate CSI ports	28 ports	38 ports	Not applicable
Number of CSI ports transitioned to permanent status	This measure keeps track of the number of ports where CSI operations have been transitioned from temporarily assigned staff to permanent staff	2 ports	15 ports	Not applicable

Source: CBP.

Appendix III: Comments from the Department of Homeland Security

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

March 22, 2005

Mr. Richard M. Stana
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
Washington, DC 20548

Re: Draft Report GAO-05-187SU, CONTAINER SECURITY: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts

Dear Mr. Stana:

Thank you for the opportunity to review and comment on the subject draft report. We are providing general comments for your use in preparing the final report and have submitted technical comments under separate cover.

The Department of Homeland Security (DHS) concurs with the draft report's three recommendations. Customs and Border Protection (CBP), a component within DHS, will evaluate the minimum level of staff assigned to foreign locations and assess staffing levels within the United States, evaluate the feasibility of requiring technical requirements for non-intrusive inspection equipment at Container Security Initiative (CSI) ports, and continue to refine, evaluate and implement performance measures. Specific actions CBP proposes to undertake to implement the recommendations are as follows:

Recommendation 1: Revise the CSI staffing model to consider (1) what functions need to be performed at CSI ports and what functions can be performed in the United States, (2) the optimum levels of staff needed at CSI ports to maximize the benefits of targeting and inspection activities in conjunction with host nation customs officials, and (3) the cost of locating targeters overseas at CSI overseas at CSI ports instead of in the United States.

CBP agrees that modifications to the CSI staffing model will allow for program objectives to be met in a cost effective manner. CBP will evaluate the minimum level of staff that would need to be assigned at a foreign location in order to maintain an ongoing dialogue with the host nation officials and ensure the integrity of the CSI operations. CBP will also assess the staffing levels that will need to be maintained at a location within the United States to support/augment CSI activities.

www.dhs.gov

2

Recommendation 2: Establish minimum technical requirements for the capabilities of noninstrusive inspection equipment at CSI ports, to include imaging and radiation detection devices, that help ensure that all equipment used can detect WMD, while considering the need not to endorse certain companies and sovereignty issues with participating countries.

CBP agrees to evaluate the feasibility of technical requirements for noninstrusive inspection equipment (imaging and radiation detection devices) at CSI ports. Since host governments purchase the equipment for use at a location outside the United States, a legal issue may exist regarding CBP's capability to impose such requirements. CBP will also seek comments and/or advice from other U.S. government agencies that would be impacted by such a decision.

Recommendation 3: Develop performance measures that include outcome-based measures and performance targets (or proxies as appropriate) to track the program's progress in meeting all of its objectives.

CBP will continue to refine, evaluate and implement any and all performance measures needed to track the progress in meeting all of CSI's objectives. This will be an ongoing activity.

We thank you again for the opportunity to provide comments on this draft report and look forward to working with you on future homeland security issues.

Sincerely,

Steven J. Pecinovsky
Acting Director
Departmental GAO/OIG Liaison

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Richard M. Stana (202) 512-8777
Stephen L. Caldwell (202) 512-9610

Staff Acknowledgments

In addition to those named above, Mark Abraham, Kristy N. Brown, Kathryn E. Godfrey, Stanley J. Kostyla, and Deena D. Richart made key contributions to this report.

Related GAO Products

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

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

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

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO-04-1062 (Washington, D.C.: September 30, 2004).

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

Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands. GAO-04-590 (Washington, D.C.: June 16, 2004).

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

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T (Washington, D.C.: March 23, 2004).

Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information. GAO-04-319R (Washington, D.C.: December 18, 2003).

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T (Washington, D.C.: December 16, 2003).

Posthearing Questions Related to Aviation and Port Security. GAO-04-315R (Washington, D.C.: December 12, 2003).

Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. GAO-03-1083 (Washington, D.C.: September 19, 2003).

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T (Washington, D.C.: September 9, 2003).

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

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions. GAO-03-902T (Washington, D.C.: June 16, 2003).

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO-03-843 (Washington, D.C.: June 30, 2003).

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T (Washington, D.C.: April 1, 2003).

Border Security: Challenges in Implementing Border Technology. GAO-03-546T (Washington, D.C.: March 12, 2003).

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T (Washington, D.C.: October 17, 2002).

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T (Washington, D.C.: August 5, 2002).

RESPONSES TO SUPPLEMENTAL QUESTIONS FOR THE RECORD
Submitted By
SENATOR NORM COLEMAN
for
THE HONORABLE ROBERT C. BONNER
Commissioner, U.S. Customs & Border Protection
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
THE CONTAINER SECURITY INITIATIVE
AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM:
SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?
May 26, 2005

1. **Recently, CBP imposed penalties on two C-TPAT members for various violations. By what method have C-TPAT members been notified that they can be penalized? Are there specific criteria to determine the length of a suspension? Does CBP maintain a list of violations and their corresponding penalties? If so, please provide this list to the Subcommittee. Is there a method by which a suspended C-TPAT member can appeal the decision? What type of due process is involved before a penalty is administered?**

In responding to this question, CBP has broken it into its component parts:

(a) By what method have C-TPAT members been notified that they can be penalized?

C-TPAT is a voluntary, incentives-based program. There are no penalty provisions associated with the C-TPAT program. Rather, penalty provisions are found in existing customs and immigration regulations. When the C-TPAT application is submitted, the agreement signed by the applicant's representative, states that the C-TPAT agreement cannot, by law, exempt the member from any statutory or regulatory sanctions in the event that discrepancies are discovered.

C-TPAT suspensions or removals may result from either negative validation findings or due to a supply chain security incident, such as a violation of the C-TPAT Agreement to Voluntarily Participate, or of existing customs and immigration regulations. In such instances, CBP exercises the enforcement discretion of the agency. Program benefits may be suspended until the identified security deficiencies are rectified; suspension may be for a set period of time or may be extended further if it is deemed necessary to ensure that the modified security measures are effective. It should be noted that although suspended from the C-TPAT program, the importer, carrier, etc., may still import and enter cargo into the United States; however, these

Permanent Subcommittee on Investigations
EXHIBIT #10

shipments will no longer receive the benefits of fewer cargo inspections and expedited cargo processing.

Recently CBP removed or suspended members from the C-TPAT program as a result of significant breaches in their supply chain security. Membership in the voluntary C-TPAT program is predicated on a commitment by the member to enhance its supply chain security measures; in exchange, CBP grants certified members the benefits of fewer cargo inspections and expedited cargo processing. When CBP discovers that the C-TPAT member has not honored their commitments to strengthen its supply chain, or in cases where a supply chain has been severely breached and compromised, CBP may suspend the program benefits afforded the member. If the findings are serious enough, the member may be removed from the program entirely, and only allowed to reapply after a specified length of time.

Suspensions and removals are not actions that CBP takes lightly. These measures will be instituted only when, after dialogue with the offending C-TPAT member, that member still fails to address the security deficiencies. At that point in the process, a decision to suspend benefits or remove a member from the program for a specified period of time is made by the program Director for routine matters. When a decision pertains to more significant or controversial matters, the Assistant Commissioner of the Office of Field Operations determines whether a certified member will be suspended or removed.

(b) Does CBP maintain a list of violations and their corresponding penalties? If so, please provide this list to the Subcommittee.

Removals or Suspensions as a Result of Validation Findings:

Importers are validated against minimum-security criteria that was adopted by CBP on March 25, 2005 and against the supply chain security measures that are documented in the security profiles that they submitted to CBP. All other C-TPAT members are validated against the security guidelines for their particular sector as well as the security measures documented in their comprehensive self-assessments submitted to CBP.

As of July 11, 2005, CBP Supply Chain Security Specialists have conducted over seven hundred validations, of which only 3.5 percent have resulted in either a suspension or removal. Specifically, reviews performed by the Supply Chain Security Specialists resulted in: the suspension of thirteen members (two importers, ten truck carriers, and one Mexican manufacturer) and the removal of twelve members (two importers, five truck carriers, and five brokers).

Removals or Suspensions as a Result of a Security Incident:

Suspensions and removals from the C-TPAT program most commonly occur as a result of a security incident where the supply chain security has been breeched or compromised. These incidents are most common along the Mexican border, and primarily affect C-TPAT truck carriers. As of July 11, 2005, there are 5,145 certified members of C-TPAT that receive benefits; notably, only 1.2 percent have had their benefits suspended or removed as a result of a security incident. Specifically, fifty-two certified C-TPAT members (fifty truck carriers, one sea carrier, and one Mexican manufacturer) have had their program benefits suspended – which include access to the FAST lanes – as a result of a security incident. Another eleven certified members (five truck carriers and six brokers / freight forwarders) have been removed from the program as a result of a security incident.

(c) Is there a method by which a suspended C-TPAT member can appeal the decision? What type of due process is involved before a penalty is administered?

Suspensions and removals from the C-TPAT program are more common as a result of a security incident where the supply chain security has been breached or compromised. When it becomes evident that the security measures have failed – for example, drugs or contraband are discovered in a member's conveyance – and a supply chain has indeed been compromised, CBP rescinds the offending member the benefits of fewer cargo inspections and/or expedited cargo processing. These incidents are most common along the Mexican border, and primarily affect C-TPAT truck carriers. A suspension may occur immediately upon discovery of a significant breach of the supply chain in order to provide the time required for CBP and the member to jointly address the security deficiencies that led to the breach, and ways to correct them. A company may be reinstated soon after a suspension if corrective measures are taken to address the security gaps. In fact, this has occurred on a number of occasions.

Where there is a narcotics seizure, CBP will immediately suspend program benefits. Thereafter, it conducts a post seizure analysis (PSA) with the C-TPAT member to determine the specific circumstances surrounding the seizure incident, and determine where the security measures broke down and were compromised. The PSA is conducted within ten days from the seizure incident, and the findings are provided to the HQ C-TPAT Office. In addition to the PSA's examination of the incident itself, a complete validation of the certified member is initiated and completed by CBP Supply Chain Specialists within thirty days of the incident. The validation reviews all security measures outlined in the submitted security profile, and provides a comprehensive assessment of the supply chain security. Weaknesses are identified and discussed with the C-TPAT member. The C-TPAT member is involved throughout this review process.

After the PSA and validations have been completed, the C-TPAT Program Director reviews the totality of the circumstances involved in the security incident, including how egregious the breach has been, and determines whether benefits should be: immediately restored; reinstated once the identified security deficiencies are rectified; or restored only after a set period of time has passed, in order to ensure that the strengthened security measures are proving effective. Suspension and removal decisions relating to routine matters are made by the Program Director. When a decision pertains to more significant or controversial matters, the Assistant Commissioner of the Office of Field Operations decides whether or not a certified member will be suspended or removed.

CBP recognizes that C-TPAT program suspensions or removals can have serious implications for certified members, yet the ability to import and enter cargo into the United States remains available to the suspended or removed member. Suspensions and removals are only initiated after dialogue with the offending C-TPAT member, and only if the member has failed to address the security deficiencies. During the entire process, the assigned CBP Supply Chain Specialist serves as the central point of contact for the C-TPAT member, ensuring continued coordination and communication between CBP and the certified company. When warranted, the program Director meets with the Supply Chain Specialist and the member's designated representatives. Members are eligible for reinstatement once all identified security deficiencies are resolved and the corrective measures are shown to be effective.

Finally, it should be noted that if a suspension occurs and there is an open enforcement action, with a possible criminal case pending, CBP is not at liberty to discuss the circumstances surrounding the case until the matter is resolved.

2. **Since the majority of shipments identified by ATS as high-risk are not inspected overseas, does CBP plan to recalibrate the ATS system for the foreign environment to ensure that ATS does not identify so many shipments as "high risk?" Alternatively, is CBP prepared to modify its claim that all high-risk shipments are searched before entering the United States?**

Under CBP's layered approach to risk management, overseas examinations are but one means through which the country's borders are protected. Because CBP can and does perform examinations domestically, overseas examinations, while extremely beneficial to U.S. safety, are not the exclusive means for protection.

There is no plan to recalibrate the Automated Targeting System (ATS) solely due to the number of examinations performed overseas. CBP does not believe it is necessary to modify its claim that all high-risk shipments are screened before entering the U.S. Through the deployment of a layered enforcement strategy; CBP currently screens 100% of all cargo that is deemed to be high risk. CBP does not

rely on any single device or technology. To identify which containers warrant further inspection, CBP employs sophisticated targeting systems, intelligence, the use of Non-Intrusive Inspection (NII) technology, the Container Security Initiative, the Customs-Trade Partnership Against Terrorism (C-TPAT), and CBP Officer experience and expertise.

3. **Do diplomatic concerns affect the manner by which C-TPAT validations are conducted overseas? Under what authority does CBP conduct these validations? Does CBP require additional authorities to assist in the implementation of its validation strategy?**

No, consent to be validated is the cornerstone of the C-TPAT program. A certified C-TPAT member will be contacted by a CBP Supply Chain Specialist (SCS) to begin the validation process. The SCSs follow internal program procedures when completing a validation. Validations verify the reliability of the materials a company voluntarily submits to CBP under the C-TPAT program, that is, the existence and effectiveness of the stated security measures. Additionally, validations provide a forum through which CBP and C-TPAT partners can build stronger partnerships by discussing supply chain security issues, sharing "best practices," and cooperatively developing solutions to address potential vulnerabilities.

C-TPAT has not been afforded access into China to conduct validations at this time.

4. **Has CBP implemented a plan for red-teaming at CSI ports? If not, how are CSI ports evaluated? What specific performance measures have been developed for CSI and C-TPAT?**

(a) Has CBP Implemented a plan for red-teaming at CSI ports? If not, how are CSI ports evaluated?

CBP has not implemented a plan for red-teaming at CSI ports. CSI ports are evaluated in three-month intervals for the first year, and every six months thereafter. Team members are evaluated on their targeting skills –that is, the facility with which they identify and examine all terrorist related high-risk shipments – and ability to interact with host government officials. ICE employees are evaluated on their ability to analyze trends and obtain intelligence to detect where maritime containers could be exploited to carry out terrorist threats.

(b) What specific performance measures have been developed for CSI?

To improve management of the Initiative, CSI has developed outcome, information and efficiency performance measures, based upon recommendations from GAO and Committee staff. In each performance measure, a series of indicators are used to

assess performance. To evaluate Outcome, CSI considers the percentage of worldwide U.S.-destined containers processed through CSI ports and the number of foreign mitigated examinations. To measure Information, CSI will review the number of: intelligence reports based on CSI foreign sources; operational CSI ports; positive findings; and investigative cases initiated due to CSI activity. Finally, efficiency is measured by the average cost per CSI port to achieve operational status.

(c) What specific measures have been developed for C-TPAT?

CBP has contracted with an outside contractor to assist in the establishment of appropriate measures and providing expert analysis. Using tools such as surveys, data collection, financial mode development and analysis, and other methods, the contractor will be able to assess the costs, benefits, and performance impacts resulting from C-TPAT participation. The benefits will be measured not only in terms of direct benefits afforded (i.e. reduced inspections and expedited processing), but also by indirect benefits, such as more efficient, predictable and transparent supply chains will also be quantified.

5. Does CBP have a plan to remedy the lack of technical or procedural standards in the Declarations of Principal that are negotiated with host nations for the CSI program?

CBP has proposed to the Government Accountability Office (GAO) to amend the Declaration of Principle (DOP). Under CBP's proposed changes, denoted in italics, the DOP would provide: "To exchange information and work together closely to help ensure the identification, screening, and sealing of high-risk containers is carried out swiftly through the use of inspection equipment that meets the specifications set forth by the World Customs Organization". This language has been accepted and used by the government of Portugal for a DOP signing on July 7, 2005.

6. Has CBP considered implementing minimum standards for inspection equipment including non-intrusive inspection technology, radiation portal monitors, and other handheld inspection tools utilized both domestically and abroad? If not, why has CBP not developed minimum standards?

On 23 June 2005, the CBP Commissioner submitted the United States' "Declaration of Intent" to adopt the World Customs Organization (WCO) "Framework of Standards to Secure and Facilitate Global Trade." This international strategy will combat terrorism and protect trade and the global economy.

The framework incorporates key elements of the U.S. strategy for securing trade and harmonizes certain customs standards and procedures among WCO members that implement the framework. These key elements are based in large measure on

initiatives designed and implemented by CBP – including the CSI program, the Trade Act and "24-Hour Rule, the Automated Targeting System developed at the National Targeting Center and used in all CSI ports by CBP personnel, and the Customs-Trade Partnership Against Terrorism (C-TPAT). Core elements of the framework are: harmonization of advance electronic manifest requirements on inbound, outbound transit shipments; a standard approach to risk management; inspection of outbound cargo using non-intrusive detection equipment; and providing tangible benefits to businesses that meet minimum supply chain security standards and implement best practices.

CSI further recommends that its counterparts in host nations purchase NII systems that follow the guidelines on page 10 of the WCO, CUSTOMS COMPENDIUM, CONTAINER SCANNING EQUIPMENT, GUIDELINES TO MEMBERS ON ADMINISTRATIVE CONSIDERATIONS OF PURCHASE AND OPERATION. This recommendation is also being incorporated in all Declarations of Principles that will be signed by all new participants in the CSI Program, beginning with Portugal (July 2005).

# # #

RESPONSES TO SUPPLEMENTAL QUESTIONS FOR THE RECORD
Submitted By
SENATOR DANIEL K. AKAKA
for
THE HONORABLE ROBERT C. BONNER
Commissioner, U.S. Customs & Border Protection
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
THE CONTAINER SECURITY INITIATIVE
AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM:
SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?
May 26, 2005

1. **Customs and Border Protection (CBP) officials have told me that the long-term goal of the Container Security Initiative (CSI) program is to do away with the stationing of CBP agents in CSI ports. However because of the partnership and trust between CBP agents and foreign customs officials, I am concerned that such a change will erase the very aspect of the program that makes it work.**

   Is it CBP's long-term plan to do away with the stationing of CBP agents in CSI ports, and if so, how do you intend to maintain a successful working relationship with foreign customs officials?

   In order to inspect all high-risk containers before they are loaded on board vessels to the United States, CBP is fostering relationships and building long-term partnerships with other countries and U.S. trading partners. CBP will also encourage interagency cooperation by developing a capacity to collect and share information and trade data gathered from CSI ports.

   CSI's initial success in developing partnerships and relationships of trust within the international customs community merits the program's continuation. Moving forward, CBP will ensure effective coordination with host countries by conducting periodic risk evaluations of ports to assess the level of staffing and other resource needs. Under the CSI program, ports are evaluated in three-month intervals for the first year and are subsequently reviewed in six-month intervals. Through the port evaluations, CBP can assess whether each CSI port has sufficient resources and the appropriate level of staffing to examine all terrorist-related, high-risk maritime containers before they are unladen in the United States. CBP believes that these periodic evaluation and assessments will provide the necessary data in order to make a sound decision of whether staffing and resources need to be reallocated.

2. **I understand that the positioning of CBP agents in foreign ports through the CSI program is just the beginning of what the Department hopes will be a global screening initiative.**

   (a) Is it true that the Department of Homeland Security (DHS) has begun discussions with other countries inviting them to send their customs representatives to U.S. ports to perform a similar function to the CSI?

   Yes, Commissioner Bonner has extended an offer to all countries currently participating in CSI to station their officers in US ports. CSI is a reciprocal program and, in accordance with the Declaration of Principle (DOP), any request for foreign customs officers to perform similar functions in U.S. ports will be considered. To date, only two countries have made such requests and those two countries are Japan and Canada.

   (b) How is this model feasible as more and more countries participate? Has CBP looked at how individual ports, such as Honolulu Harbor for example, would host a number of international customs teams at their facilities?

   To date, only Japan and Canada have requested that their customs officers be stationed at a U.S. port. The Japanese customs officers are stationed in Long Beach, California; Canadian customs representatives are located in Seattle, Washington and Newark, New Jersey. Stationing of additional foreign customs officers in U.S. ports would be discussed with the prospective foreign government and would include discussions on what ports in the U.S. would be most appropriate for stationing foreign officers. As a criterion for requesting their customs officers be stationed at a particular U.S. port, participating foreign customs administrations would look to ports that have the most volume of maritime containers that leave a U.S. port with direct shipment to their port.

3. **To enhance customs screening and border protection, the World Customs Organization maintains a database into which member countries feed information regarding customs violations. European officials tell me that although the United States utilizes information from the database, the U.S. does not contribute data.**

   Since DHS increasingly relies on America's allies to help secure cargo headed for the U.S. and to track and circumvent illegal shipping activities abroad, should the United States share information on customs violations with its international partners?

   U.S. Customs and Border Protection exchanges information with other countries to support enforcement actions aimed at cracking down on illegal activities through various customs to customs contacts. This includes providing information on

violations identified by CBP through actions to enforce customs laws and protect our borders. In coordination with U.S. Immigration and Customs Enforcement, CBP also provides information as needed to support investigations into criminal activities.

To supplement information exchange process, CBP is currently working towards participation in the World Customs Organization (WCO) on-line database. This participation will make more information on seizures made at U.S. borders available to WCO member countries. While participation by WCO members in sharing information through the database has been somewhat limited, U.S. participation may lead to increased sharing of information by other countries.

4. If a CSI team identifies a container as high-risk for reasons other than terrorism, drug smuggling for example, what action would they take?

The principal mission of CSI teams based overseas is to screen container shipments that are identified as a high terrorist risk. However, CSI officers may encounter shipments that involve criminal activity not directly related to this primary mission. If the CSI officers encounter the information through normal targeting procedures, the officers then notify their host nation counterparts, who, in turn, may request that the container be inspected. If the host nation decides to not ask for an inspection, the CSI officers then enter remarks in the notes section of the Automated Targeting System that would alert the U.S. port of arrival of a suspect container. In addition, the CSI officers may also alert personnel at the National Targeting Center (NTC), which would then coordinate an inspection of a container in the United States.

If evidence of criminal activity is discovered during the actual inspection (NII or physical), CSI officers notify the local ICE Attaché and the customs agents of the host nation. The ICE Attaché and/or host nation may decide to pursue the case, depending on the infraction. On several occasions, CSI teams have alerted their host nation counterparts to the presence of smuggled cigarettes, after receiving this information from the local ICE Attaché. For example, in June 2003, the CSI team in Felixstowe, England notified Her Majesty's Customs and Excise (HMCE) to the presence of over two million counterfeit Marlboro cigarettes in a container of furniture.

# # #

RESPONSES TO SUPPLEMENTAL QUESTIONS FOR THE RECORD
Submitted By
SENATOR PETE DOMENICI
for
THE HONORABLE ROBERT C. BONNER
Commissioner, U.S. Customs & Border Protection
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
THE CONTAINER SECURITY INITIATIVE
AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM:
SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?
May 26, 2005

Commissioner Bonner, as you know, adequate staffing at our nation's land ports of entry is essential for the safety of parties involved in the flow of traffic across the border and for efficient commerce.

Last year's legislation that reorganized our intelligence community called for an increase in border patrol agents, and President Bush's FY 2006 budget requests funds to hire an additional 210 agents.

1. **Have you studied where placing these agents would be most beneficial?**

   Yes, the Office of Border Patrol (OBP) has a national strategy that addresses the deployment of new assets to high priority sectors. While the majority of new Border Patrol Agents will go to the El Paso Sector in Fiscal Year 2005, new agents will also be sent to Yuma and Tucson.

2. **When might these new agents be hired and put in place?**

   CBP is continuously engaged in the recruitment and hiring of new border patrol agents, some of whom are currently enrolled in the Academy and others are in various phases of the hiring process. For Fiscal Year 2006, CBP's Office of Border Patrol has developed a new, proactive recruiting campaign, announced July 1, 2005, that is presently being implemented. CBP's recruitment efforts include visiting military bases and colleges, increasing advertising and expanding public awareness campaigns through the Internet and public service announcements, and expediting the hiring process through "Compressed Testing" sites at high volume locations along the southwest border.

# # #

RESPONSES TO SUPPLEMENTAL QUESTIONS FOR THE RECORD
Submitted By
SENATOR DANIEL K. AKAKA
for
RICHARD M. STANA
Director, Homeland Security & Justice Team
Government Accountability Office

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
THE CONTAINER SECURITY INITIATIVE
AND THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM:
SECURING THE GLOBAL SUPPLY CHAIN OR TROJAN HORSE?
May 26, 2005

Question 1: Given that the CSI program is dependent on the cooperation of the host government, do you believe CSI can be successfully implemented in countries that have significantly lower security standards and fewer screening resources than the United States?

Response 1: CBP has minimum requirements for a host government to participate in the CSI program. To become a CSI port, CBP requires that (a) the port has regular, direct, and substantial container traffic to ports in the United states; (b) the host government customs officials must be able to inspect cargo originating, transiting, exiting, or being transshipped through a country; and (c) the host government must have nonintrusive inspection equipment and radiation detection equipment available for use at or near the port. In addition, CBP also requires that participating CSI ports commit to (1) establishing an automated risk management system; (2) sharing critical data, intelligence, and risk management information with CBP; (3) conducting a thorough port assessment and commit to resolving port infrastructure vulnerabilities; and (4) maintaining employee integrity programs and identify and combat beeches in employee integrity. Many host governments and ports that meet these minimum requirements might have lower security standards and resources than the United States. Nevertheless, it could be useful to CBP to include such governments and ports in the CSI program. First, containers used to transport WMD could originate anywhere and be shipped via circuitous routes—so additional port coverage may be advantageous. In addition, host governments in the Middle East and Africa might have access to more useful information on terrorists intentions and operations than some of the existing CSI host governments. If host government security standards and resources at a CSI port appear to be inadequate or poorly applied for selected containers, CBP can always decide to inspect such containers again at the U.S. port of arrival.

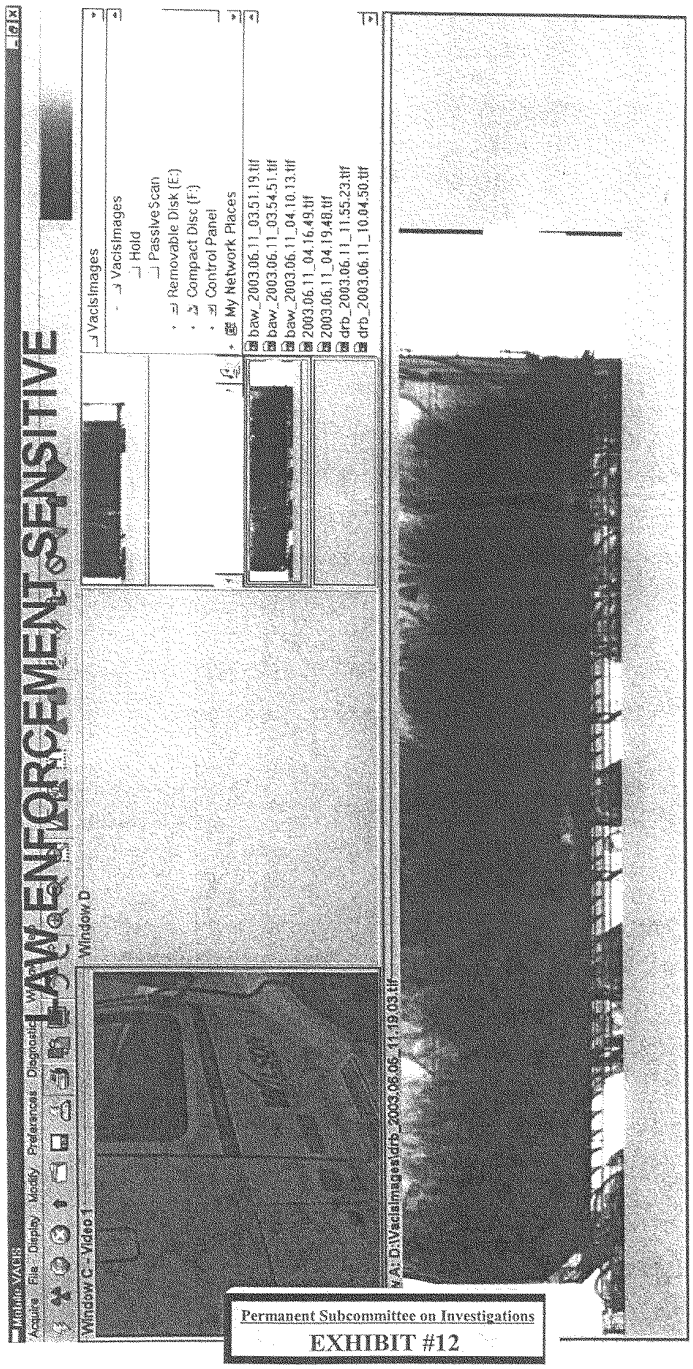
Permanent Subcommittee on Investigations
EXHIBIT #11

Question 2: Given your analysis of the CSI program, do you think it is an advisable goal or do you believe there will always be a need for a CBP presence in foreign ports to ensure that CSI functions properly?

Response 2: Our analysis indicated that many of the CSI personnel posted overseas at some CSI ports were not directly dealing with host government officials. These personnel were conducting activities—such as reviewing targeting data and consulting databases—that could be accomplished in the United States. However, we also noted benefits from having personnel located at the CSI ports and these benefits would be lost if all CSI personnel were withdrawn. For example, some CSI team personnel have daily face-to-face interaction with host government officials at ports to share information and observe inspections. Our report recommended that CBP revise the CSI staffing model to consider (1) what functions need to be performed at CSI ports and what functions can be performed in the United States, (2) the optimum levels of staff needed at CSI ports to maximize the benefits of targeting and inspection activities in conjunction with host government customs officials, and (3) the costs of locating targeters overseas in CSI ports instead of the United States.

Question 3: Do you agree with the assertion that some CSI ports do not comply with the minimum standards set by CBP to become a CSI port, and if so, what action, if any, does CBP take to address the port's failure to comply?

Response 3: As detailed in our response to question 1, CBP has minimum requirements for a host government to participate in the CSI program. Our work at four CSI ports found no indications that host governments and ports did not comply with CBP requirements. While these minimum standards do not require that CSI ports operate on par with U.S. port security standards, CBP believes they provide reasonable assurance that the CSI program can be successfully implemented at a port. Our work did note that different CSI ports are using different nonintrusive inspection equipment, and our report recommended that CBP establish minimum technical requirements for the capabilities of such equipment.



Permanent Subcommittee on Investigations

EXHIBIT #12