

**SUPPLY CHAIN SECURITY: SECURE FREIGHT
INITIATIVE AND THE IMPLEMENTATION OF
100 PERCENT SCANNING**

HEARING

BEFORE THE

SUBCOMMITTEE ON SURFACE TRANSPORTATION
AND MERCHANT MARINE INFRASTRUCTURE,
SAFETY, AND SECURITY

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 12, 2008

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

80-493 PDF

WASHINGTON : 2013

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) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

DANIEL K. INOUE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, <i>Vice Chairman</i>
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
BARBARA BOXER, California	OLYMPIA J. SNOWE, Maine
BILL NELSON, Florida	GORDON H. SMITH, Oregon
MARIA CANTWELL, Washington	JOHN ENSIGN, Nevada
FRANK R. LAUTENBERG, New Jersey	JOHN E. SUNUNU, New Hampshire
MARK PRYOR, Arkansas	JIM DEMINT, South Carolina
THOMAS R. CARPER, Delaware	DAVID VITTER, Louisiana
CLAIRE McCASKILL, Missouri	JOHN THUNE, South Dakota
AMY KLOBUCHAR, Minnesota	ROGER F. WICKER, Mississippi

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*

LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*

CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*

PAUL NAGLE, *Republican Chief Counsel*

SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT
MARINE INFRASTRUCTURE, SAFETY, AND SECURITY

FRANK R. LAUTENBERG, New Jersey, <i>Chairman</i>	GORDON H. SMITH, Oregon, <i>Ranking</i>
JOHN D. ROCKEFELLER IV, West Virginia	JOHN MCCAIN, Arizona
JOHN F. KERRY, Massachusetts	KAY BAILEY HUTCHISON, Texas
BYRON L. DORGAN, North Dakota	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	JIM DEMINT, South Carolina
MARK PRYOR, Arkansas	DAVID VITTER, Louisiana
THOMAS R. CARPER, Delaware	JOHN THUNE, South Dakota
CLAIRE McCASKILL, Missouri	ROGER F. WICKER, Mississippi
AMY KLOBUCHAR, Minnesota	

CONTENTS

Hearing held on June 12, 2008	Page 1
Statement of Senator Lautenberg	1

WITNESSES

Ahern, Jayson, Deputy Commissioner, U.S. Customs and Border Protection, U.S. Department of Homeland Security	2
Prepared statement	5
Caldwell, Stephen L., Director, Homeland Security and Justice Issues, U.S. Government Accountability Office (GAO)	16
Prepared statement	18
Huizenga, David, Assistant Deputy Administrator, Office of International Material Protection and Cooperation, Defense Nuclear Nonproliferation, National Nuclear Security Administration, U.S. Department of Energy	9
Prepared statement	11

APPENDIX

American Association of Exporters and Importers, prepared statement	41
Response to written questions submitted by Hon. Maria Cantwell to:	
Stephen L. Caldwell	55
Response to written questions submitted by Hon. Frank. R. Lautenberg to:	
Jayson Ahern	48
David Huizenga	52
Robinson, Catherine, Associate Director, High Technology Trade Policy on behalf of the National Association of Manufacturers (NAM), prepared state- ment	46
Stein, Renee, Chair, and Richard M. Belanger, Counsel, Business Alliance for Customs Modernization, prepared statement	45

SUPPLY CHAIN SECURITY: SECURE FREIGHT INITIATIVE AND THE IMPLEMENTATION OF 100 PERCENT SCANNING

THURSDAY, JUNE 12, 2008

U.S. SENATE,
SUBCOMMITTEE ON SURFACE TRANSPORTATION AND
MERCHANT MARINE INFRASTRUCTURE, SAFETY, AND SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:05 a.m., in room SR-253, Russell Senate Office Building, Hon. Frank R. Lautenberg, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Good morning. I call the Surface Transportation and Merchant Marine Infrastructure, Safety, and Security Subcommittee to order.

Welcome. We thank the witnesses for being here and all of you for your attention to this very serious problem. I want to welcome everyone to today's hearing as we continue America's work to protect our families, protect our communities, protect our economy by securing our ports and those containers that arrive there.

Now, my home state of New Jersey knows about the importance of ports. The Port of New York and New Jersey is the largest port on the east coast and the second busiest container port in the country. It supports some 250,000 jobs and is responsible for generating \$20 billion in economic activity.

The 40-foot metal shipping containers, which have become standard for industry, were first used in the United States at Port Newark, New Jersey, and today these containers have transformed global commerce. They save manufacturers and shippers time by moving goods more efficiently and with less expense.

But after 9/11, we were forced to see these containers in a different light, as a way for terrorists to smuggle weapons or themselves into our country. An attack on a U.S. port or even a foreign port would affect our economy, not to mention the safety of surrounding communities. To prevent that from happening and to keep our country safe, we need to know what is in these containers.

The Bush Administration has long believed that a layered approach is adequate for securing our ports. I would consider it a modular approach, but in practice, this layered approach has been

more like a piecemeal one, leaving our country and our economy still vulnerable.

After the 9/11 attacks, the Federal Government installed equipment to scan 100 percent of passengers and baggage boarding a plane. It should not take another attack on our country for the Federal Government to secure our ports.

To that end, Congress passed a law last year requiring that by year 2012, all shipping containers coming into our ports should be scanned for nuclear weapons and radiation before they reach our shores. It is my understanding that today's administration witnesses are about to tell us that July 2012, the deadline, will not be met.

The GAO has already told Congress twice this year that the Bush Administration's cargo security programs are riddled with loopholes. For example, we still do not have minimum standards for container security. The Department of Homeland Security still has not established a standard lock for metal shipping containers, and I am deeply concerned that more than 6 years after 9/11, the Bush Administration is back once again to report on more problems. The administration's approach to securing our ports is unacceptable, and while they get the technology in place for 100 percent scanning, we also need to find additional ways to increase security at our ports.

To that end, I will soon introduce legislation which will make real improvements to our port security programs and keep our economy and families safe.

I look forward to hearing from our witnesses on these critical issues. I thank you for being here. I would ask that Jayson Ahern, who is the Deputy Commissioner for U.S. Customs and Border Protection, be the first to speak. Mr. Ahern has spent 32 years in public service, and I want to thank you for your commitment to the country.

We will, after that, hear from David Huizenga, Assistant Deputy Administrator at the U.S. Department of Energy. At the Department, Mr. Huizenga is responsible for the Second Line of Defense Program, which includes maritime security and the Megaports initiative.

Stephen Caldwell is the Director of Maritime Security Issues at the U.S. Government Accountability Office, and he has written GAO reports on maritime legislation such as the SAFE Port Act and the issues of port security and container security.

So, once again, I thank each of you for joining us today, for sharing your expertise with us. Mr. Ahern, if you will, please. It is a 5-minute rule, as you know. Please give us your testimony.

STATEMENT OF JAYSON AHERN, DEPUTY COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. AHERN. Good morning Chairman Lautenberg, and thank you very much for this opportunity to discuss the Secure Freight Initiative, or SFI, and the recently released report on the pilot ports.

First of all, I want to apologize to you and the rest of the Committee and the staff for providing this report so late in the process and after the April deadline, but we wanted to make sure the infor-

mation we provided was as complete and as thorough as possible and we wanted to include the reviews of our trade and our international partners as well.

I also want to thank the Members of this Committee for your strong support of Customs and Border Protection as we work to continue to provide the protection our nation is so necessarily in need of. This Committee has been instrumental in the success of CBP's cargo security strategy, as well as the passage of the SAFE Port Act, which in itself represents an impressive collaboration between the Congress and the Administration to protect our nation.

In addition to requiring the SFI ports, the SAFE Port Act codified a number of CBP supply chain security programs, specifically our advance information requirements and automated targeting systems, the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, and the use of nonintrusive inspection technology to scan high-risk shipments. These provisions reflect strong support for our current layered risk-based approach to maritime and cargo security.

We continually point out that the layers of the strategy are interdependent, different layers focus on securing different parts of the supply chain. This ensures that cargo is regularly assessed and that security does not rely on one single point that could be easily compromised. Over the last several years, we have dedicated significant resources to our cargo and port security programs and this has resulted in a strong risk management approach.

I am concerned, however, that while we continue to increase resources for an initiative like SFI, we may be neglecting other areas that could potentially pose a greater risk to the country. While increased resources for programs such as SFI have enhanced our ability to address maritime container security vulnerabilities, it is important to recognize that 100 percent scanning does not equal 100 percent security. Risk management and security must be driven by our informed judgment and totality of the risks.

As directed by the Congress, last October we began testing the feasibility of scanning 100 percent of U.S.-bound containers in three SFI ports, in Honduras, Pakistan, and the United Kingdom. From October to May of this year, we scanned over 170,000 containers passing through these ports to the United States.

Under SFI, an integrated scanning system, consisting of radiation portal monitors provided by the Department of Energy and nonintrusive inspection imaging systems provided by Customs and Border Protection, scans containers as they move through the foreign ports. The data from the SFI systems provide additional data points that are used in conjunction with the advance manifest information such as the 24-hour rule, C-TPAT, and our automated targeting system so we can assess the totality of the risk in each container coming to the United States.

CBP and the Department of Energy are true partners, and my counterpart, Mr. Huizenga, as a trusted colleague in the Megaports program, has brought invaluable resources and institutional knowledge to our effort.

As our report will show, we learned important lessons, both positive and negative, from the pilots.

On the positive side, we benefited from considerable host nation cooperation, low transshipment rates, as well as technology and infrastructure, paid for primarily by the U.S. Government, but we also recognize that such accommodations and supportive conditions do not and will not exist in all ports shipping to the United States.

The pilots also demonstrated that integrated imaging and radiation detection equipment can produce useful data. The additional data elements gathered at the foreign ports assist Customs and Border Protection officers in mitigating risk and resolving radiation alarms at a domestic seaport. This results in enhanced data collection and more effective trade facilitation.

But on the negative side or the side that presents the greatest challenges, even with favorable conditions, we found that deploying container scanning equipment at each of the SFI ports has presented certain operational, technical, logistical, financial, and diplomatic challenges, including reconfiguring port layouts to accommodate the equipment without affecting port efficiency, identifying who will incur the cost for operating and maintaining the scanning equipment, concluding agreements with partnering nations and terminal operators, and staffing implications for the foreign customs service and terminal operators.

But I would submit the most important and challenging issue facing SFI is finding an effective and meaningful way to scan transshipped containers. The initial pilots demonstrated that technological and operational solutions are not yet available to capture transshipped cargo efficiently. New equipment and software must be developed to overcome the considerable challenge of scanning containers that often transit through ports quickly and without necessarily being placed on trucks or passing through the front gates. So while additional data can be useful, challenges and expenses are significant even in these limited environments.

As a result of what we have learned so far, Customs and Border Protection will focus future scanning deployments on high-risk trade corridors since they pose the greatest threats to the United States, prioritizing these deployments in a way which will maximize the security benefit, and ensure that we have the capacity to integrate the additional scan data into our risk-based strategy. Considering the approximate 11.5 million containers in a maritime environment that enter the United States annually, it is imperative that resources remain focused on securing global commerce without interrupting the flow of legitimate goods. To ensure these twin goals of trade facilitation and security, CBP will continue to employ a layered risk-based approach to security. Our judgments will be based on the totality of risk we face from potentially dangerous goods and people entering our nation.

Over the last several years, we have devoted much discussion and effort to container security, but with our layered defense strategy in place, we believe we must devote equal energy and resources to other potential threats to U.S. ports and other areas along our borders in the supply chain.

Thank you very much for the opportunity and I look forward to dialogue on this issue with you today.

[The prepared statement of Mr. Ahern follows:]

PREPARED STATEMENT OF JAYSON AHERN, DEPUTY COMMISSIONER, U.S. CUSTOMS
AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Introduction

Chairman Lautenberg, Ranking Member Smith, and distinguished Members of the Subcommittee:

Good morning and thank you for this opportunity to discuss the Secure Freight Initiative (SFI) and the recently released report on the initial pilot ports. I want to take this opportunity to apologize for submitting the report past the April deadline. We wanted to ensure that the report was as robust as possible and have worked hard to provide a comprehensive assessment of the progress made at each of the seven locations, detail the challenges and successes, and outline the future strategy for the deployment of integrated scanning technology abroad.

I want to thank the Committee for its strong support of CBP. This Committee played a central role in the passage of the Security and Accountability for Every Port (SAFE) Act of 2006, legislation that directed the Department of Homeland Security (DHS) to explore, on a pilot basis, the feasibility and potential benefits of an international scanning program at three foreign ports. I look forward to reporting back to you on our experiences during these pilots and on some of the lessons we have learned.

I would also like to take the opportunity to thank the foreign governments and customs officials that have partnered with us throughout this process, as well as the port and terminal operators and other stakeholders whose support and collaboration was indispensable. The SFI pilots have benefited from host nation officials and port operators willing to expend, to varying degrees, the resources associated with additional staffing, alarm response protocols, construction and other infrastructure upgrades. Importantly, this report also includes input from these industry and foreign government partners.

Before discussing the SFI program, I must note that the success of CBP's cargo security strategy stems from a risk-based, layered enforcement approach. It includes advance information, sophisticated technology, and partnerships with the trade community and other countries. In addition to requiring the SFI pilots, the SAFE Port Act supported the current layered, risk-based approach to maritime and cargo security by codifying a number of supply chain security programs that DHS established following the September 11, 2001 terrorist attacks and which continue today. Specifically, the SAFE Port Act codified DHS' advanced information requirements and automated analysis, the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), and the use of non-intrusive inspection (NII) technology to scan high-risk shipments.

These programs form the backbone of CBP's risk-management, layered enforcement strategy. To most effectively manage multiple threats to our country, we must direct resources to areas of greatest risk. We are constantly working to refine this layered process by strengthening our tools and capabilities, working to maintain an appropriate balance between the wide range of threats we face and allocating our limited resources accordingly. It is important to reiterate that the layers of this strategy are interdependent and that different layers secure different parts of the supply chain. This approach ensures that cargo is regularly assessed and that security does not rely on any single point that could be compromised.

Although there has been much discussion about maritime container security in recent years, we have also been—and must remain—focused on other threats to our borders and to other components of the supply chain. We must remain vigilant in securing all conveyances and in screening passengers at our land borders, airports, railways, and small vessel terminals. In fact, although we frequently refer to the 11.5 million containers arriving by sea, there are an equal number of truck containers arriving across our land borders with Canada and Mexico.

While increased resources for programs such as SFI have enhanced our ability to address maritime container security vulnerabilities, it is important also to recognize that 100 percent scanning DOES NOT equal 100 percent security and that no single layer or tool in our risk-based approach should be overemphasized at the expense of the others. The strength of the strategy is that it ensures continuous security at multiple nodes in the supply chain, distributing resources so that focus on one threat does not overshadow other vulnerable areas that could also be exploited.

The Secure Freight Initiative (SFI)

Now I'd like to turn my attention to the international integrated scanning program under the Secure Freight Initiative (SFI).

Under SFI, an integrated scanning system, consisting of radiation portal monitors (RPM) provided by DOE/National Nuclear Security Administration and non-intru-

sive inspection (NII) imaging systems provided by CBP, is used to scan containers as they move through the pilot locations in the foreign ports. Through optical character recognition (OCR) technology, data from these systems is integrated and provided to CBP officers who can use it, along with customary data sources, to determine if the container should be referred to the host nation for secondary examination prior to being loaded onto a vessel destined for the United States. SFI provides additional data points used by CBP officers in conjunction with advanced manifest data, such as 24-hour rule information, Customs-Trade Partnership Against Terrorism (C-TPAT) information, and the Automated Targeting System (ATS) to identify high risk containers that warrant additional scrutiny prior to continuing on through the global supply chain.

Meeting the legislative requirements of the SAFE Port Act, the first three SFI ports (Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom) became fully operational on October 12, 2007. Under SFI, DHS and DOE work to scan all U.S.-bound maritime containers; the total U.S.-bound container volume at these three ports from October 12, 2007 to May 25, 2008 was 170,564 containers. Furthermore, CBP and DOE are working to pilot scanning equipment in additional complex environments, such as high-volume and transshipment ports. These additional locations include certain terminals in Hong Kong (which is now fully operational); Salalah, Oman and Port Busan, South Korea.

With the three initial SFI pilot ports in Honduras, the United Kingdom, and Pakistan, CBP has focused its efforts on exploring methods by which efficient operation (defined as maximizing the security benefit, minimizing disruptions to port operations, and containing costs) could be achieved within the deadline prescribed by law (the SAFE Port Act and the 9/11 Act). The SFI deployments in Honduras, the United Kingdom, and Pakistan indicate that scanning U.S.-bound maritime containers is possible on a limited scale.

However, SFI operations in these initial locations benefited from considerable host nation cooperation, low transshipment rates, and technology and infrastructure costs covered primarily by the United States Government—accommodating and supportive conditions that do not exist in all ports shipping to the United States.

As will be discussed in more detail, the data obtained by the scanning technology does have the potential to enhance targeting by providing two additional data points (RPM spectra and NII images) to the information and tools already available to CBP officers. CBP is committed to a realistic and responsible approach that will incorporate these scan data points into our risk-based methodology in places where the additional information would be of the most benefit to our targeters.

SFI Challenges

The pilots have demonstrated that not just scanning equipment, but a combination of technology, processes, and collaboration is necessary to a successful scanning system; additional necessary factors include innovative solutions to operational hurdles, useful data that is collected, analyzed and primed to enhance targeting, a collaborative approach with the international community and port operators, and perhaps most importantly, responsible and practical policies informed by the totality of the threats to which the U.S. remains vulnerable.

The continuation of operations in some of the current SFI pilot locations will afford CBP the opportunity to further test possible solutions to the complex challenges posed by transshipment and high-volume ports. While we continue to learn important lessons in these initial pilot locations, CBP will focus future scanning deployments on high-risk trade corridors that represent the greatest threats to the United States. Prioritizing deployments in this way will maximize the security benefit that can be achieved with limited departmental funds and ensure that CBP has the capacity to compile, assess, and integrate the additional scan data into its effective, functioning risk-based strategy.

Thus far, the deployment of container scanning equipment at each of the SFI ports has presented certain operational, technical, logistical, financial, and diplomatic challenges that will likely continue to be encountered, to varying degrees, as SFI deploys to additional locations. These challenges include:

- Sustainability of the scanning equipment in extreme weather conditions and certain port environments;
- Varying costs of transferring the data back to the United States (National Targeting Center) in real-time, etc.;
- Re-configuring port layouts to accommodate the equipment without affecting port efficiency;
- Developing local response protocols for adjudicating alarms;

- Addressing health and safety concerns of host governments and respective trucking and labor unions;
- Identifying who will incur the costs for operating and maintaining the scanning equipment;
- Acquiring necessary trade data prior to processing containers through the SFI system;
- Addressing data privacy concerns in regards to the scanning data;
- Concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as: ownership, operation, and maintenance of the equipment; sharing of information; and import duty and tax considerations;
- Staffing implications for both the foreign customs service and terminal operator;
- Licensing requirements for the scanning technology;
- Reaching agreement with foreign and industry partners to continue scanning 100 percent of U.S.-bound containers after the pilot ends; and
- Discussing the potential requirements for reciprocal scanning of U.S. exports.

While these challenges are consistent at our pilot ports, the remedies must be specifically tailored to the unique characteristics of each port. One example of a challenge requiring different fixes in each location was the different level of automation, with paper-based rather than computerized systems, in some of the initial SFI ports. In many situations, containers can arrive at the port up to several days before they are loaded on vessels. If containers arrive more than one day before lading, then CBP will not yet have the container's corresponding trade information, received under the 24-hour rule. Without information about what is in the container or whether it is U.S.-bound, resolving an RPM alarm or image anomaly is more difficult. CBP addressed this challenge in a variety of ways, including agreements with customs partners, terminal operators, and carriers for access to certain information (such as destination and commodity descriptions to identify U.S.-bound containers) that assisted with the risk assessment process and adjudication of radiation alarms. Those ports that lack an automated system will provide additional challenges for providing manifest and destination information to CBP.

One challenge has proven particularly difficult to overcome: operating these systems in a transshipment port. The initial SFI pilots have demonstrated that technical and operation solutions are not yet available to capture transshipped cargo efficiently. New equipment and software must be developed to address the considerable challenge of scanning containers that often transit through ports quickly and without necessarily being placed on trucks or passing through port gates. To date, SFI has progressed on a limited scale in ports that take advantage of the natural chokepoints of entry and exit gates to scan containers. This approach typically prevents significant impact on port operations, but is not applicable in heavy transshipment ports where containers arrive on one ship and depart on another without entering or exiting through the port gates. Because of shorter dwell times for containers, space constraints, lack of immediate availability of shipping data, and the difficulty of identifying chokepoints within busy container terminals, capturing transshipped cargo without seriously impacting port operations remains a significant challenge. Solutions to this challenge will depend upon the specific infrastructure conditions at any given port, technology interface issues, and the development of operational procedures in concert with host nation and port officials. Advances in technology that require a smaller physical footprint are also essential to any future large-scale implementation of SFI.

The initial deployments under SFI also demonstrate the significant costs associated with procuring and deploying scanning technology and the supporting information technology (IT) infrastructure. With the announcement of SFI in 2006, DHS and DOE each committed approximately \$30 million toward the implementation of SFI at the initial three ports and the installation of equipment at three additional ports where integrated scanning is to be demonstrated on a limited scale.

Costs to industry and foreign partners were minimized during the initial SFI pilot by the use of primarily U.S.-owned systems in SFI ports, as well as U.S.-funded upgrades to terminal operating systems (TOS) and enhancing the local IT infrastructure. In addition to costs incurred by the U.S. Government associated with SFI scanning, the terminal operators are also absorbing costs in the form of fuel for the trucks, time to run containers through the systems, and utilities. With the exception of Puerto Cortes, terminal operators do not presently assess a fee to recoup their costs; however, they may begin to do this after the pilot phase. Additionally, our for-

foreign Customs partners are absorbing costs associated with increased staffing levels including overtime, training, and personnel assigned to full-time operations.

Although DHS and DOE funded the initial phase of SFI deployments, the equipment, IT, and personnel costs associated with expanding the program to cover all U.S. bound traffic from the more than 700 different ports that ship to the United States—some significantly larger and more complex than any of the first three pilots—means that the benefit of immediate widespread deployments must be weighed against the Department's funding needs to address other homeland security priorities.

While RPM spectra and NII images can be useful additional data points for evaluating the risk of U.S.-bound containers, the lack of universal solutions to make scanning cost-effective and efficient in every port underlies the Department's strategy to focus future SFI deployments on trade corridors that present the highest risk. Gathering scan data from these high risk corridors will provide additional information, consistent with the Department's successful layered strategy, for CBP targeters, enhancing risk assessments in the most vulnerable areas without overwhelming the Department's budget, personnel resources, and ability to defeat other serious threats to the homeland.

SFI Benefits

While highlighting many challenges, the SFI pilots have also produced valuable and positive feedback. SFI, in the initial three ports, has demonstrated the operational feasibility of integrating various scanning technologies and transmitting large amounts of data in near-real time for review and analysis. SFI has also demonstrated that scanning data associated with maritime containers at a port of lading can be integrated into CBP's ATS and reviewed alongside the targeting system's risk assessment rule sets. This information can be successfully integrated by electronically linking specific container identification data to that container's scanning data. To date, CBP has successfully integrated, transmitted, and received thousands of data files from the three operational ports.

Additionally, a preliminary analysis of the potential trade facilitation benefits of SFI has been positive. Containers arriving in the United States accompanied by SFI data do not experience the same rate of examination at U.S. ports as containers that originate from non-SFI locations. As well, the additional data elements gathered at the foreign port assist CBP officers in more quickly and efficiently mitigating risk and adjudicating radiation alarms occurring at a domestic seaport.

SFI Potential Operation in Additional Ports

As noted earlier, the implementation of SFI in Pakistan, Honduras, and the United Kingdom, and the limited testing in the four other SFI locations, illustrates that the scanning of all U.S.-bound maritime containers in a foreign port is possible on a relatively contained scale. As DHS, in conjunction with the DOE and the DOS, develops a specific policy forward, we will prioritize our resources and efforts by focusing on specific higher risk trade corridors where the most security benefit can be realized. Based on preliminary results from the three pilot locations, and in light of the considerable costs and challenges associated with the deployment of SFI/ICS systems, this high risk trade corridor approach accords with the current risk-based strategy, best addresses the greatest threats to the United States, and represents the most worthwhile investment of limited available resources for the scanning of cargo containers at foreign ports.

The issue of container security has precipitated much discussion and effort over the last several years, but the Department has also been, and must remain, attuned to other threats to U.S. ports and other potentially vulnerable components of the supply chain. DHS and Congress have dedicated significant resources and efforts to our cargo and port security programs which have been instrumental in the development of the robust layered and risk-management approach currently in place. We are always eager to enhance these layers and even further refine our targeting to ensure that we focus on those goods and people that represent a threat to our nation. I'm concerned, however, that while we continue to increase resources specifically for container security initiatives, like SFI, we could be neglecting other areas of concern that potentially pose greater risk and vulnerability to the country. Again, a risk management approach to security has to be driven by our informed judgment about the totality of potential risks to the country, not just risks to a single vector.

Furthermore, traffic congestion brought upon by the movement of shipping containers is a threat to the global economy. The United States is especially vulnerable since over 90 percent of its imports and exports move via sea container. As a nation, and as a global trading partner, we must prioritize our security efforts to embrace the principle "to facilitate the movement of commerce", and align security programs

with those efforts that enhance cargo flow through the supply chain in a transparent and accountable process. In this way, transportation providers may be more effective and efficient in protecting our prosperity and those of other trading partners.

Thank you again for this opportunity to testify. I look forward to having a dialogue with this Subcommittee on the merits and future of container scanning.

Senator LAUTENBERG. Thank you very much, Mr. Ahern.

Now, do you pronounce your name Huizenga or Huizenga?

Mr. HUIZENGA. The former, Mr. Chairman. Huizenga.

Senator LAUTENBERG. Yes, the hockey team owner and that kind of thing?

Mr. HUIZENGA. Yes. I am not sure if I am a distant relative of Uncle Wayne. It is not clear.

Senator LAUTENBERG. It is worth the search.

[Laughter.]

Mr. HUIZENGA. We could start a rumor I guess.

[Laughter.]

Senator LAUTENBERG. Welcome and we invite you to give your testimony.

**STATEMENT OF DAVID HUIZENGA, ASSISTANT DEPUTY
ADMINISTRATOR, OFFICE OF INTERNATIONAL MATERIAL
PROTECTION AND COOPERATION, DEFENSE NUCLEAR
NONPROLIFERATION, NATIONAL NUCLEAR SECURITY
ADMINISTRATION, U.S. DEPARTMENT OF ENERGY**

Mr. HUIZENGA. Thank you, Chairman Lautenberg, for the opportunity to be here today, along with Deputy Commissioner Ahern and the General Accounting Office to address this important issue.

I am here to discuss the Department of Energy's role in the Secure Freight Initiative, which is a partnership with the Department of Homeland Security's Customs and Border Protection and the State Department. I will highlight recent progress in our efforts to thwart nuclear terrorism, as well as discuss key challenges to accelerating and expanding radiation scanning of U.S.-bound containers at foreign seaports, as required by the SAFE Port and 9/11 Acts.

For the last 15 years, my office has focused on securing nuclear materials and weapons at well over 100 facilities in Russia and other states of the former Soviet Union. This is the first line of defense in a strategy to deny terrorists access to fissile materials, or the essentials elements of a nuclear weapon. We are scheduled to complete the vast majority of the security upgrades at these facilities by the end of 2008.

As a natural complement to these efforts, in 1998 we established the Second Line of Defense Program, or the SLD program. As part of the defense-in-depth strategy to protect the U.S. homeland from attack by a nuclear or radiological device, the SLD program provides equipment and training to foreign authorities to help them detect, deter, and interdict illicit trafficking in nuclear and other radioactive materials. To date, we have installed over 1,000 radiation portal monitors at over 160 sites, including vehicle, rail and pedestrian border crossings, airports and seaports.

The Second Line of Defense's Megaports Initiative was launched in 2003 to address the possibility of nuclear trafficking in the global maritime shipping system. Megaports is focused on radiation

scanning of containerized cargo, including imports, exports, and transshipments, regardless of the destination of the cargo. Based on research and modeling that takes into account both shipping volume and regional threat, Megaports has identified approximately 75 ports of interest to be equipped by 2013, which would constitute over 50 percent of the global shipping traffic. We have made strong progress toward this goal. We are operational in 12 ports and in various phases of implementation and engagement in 27 others.

For several years, the Megaports program has partnered with CBP on its Container Security Initiative, which led naturally to working together on the Secure Freight Initiative. In support of the SFI, we provided radiation detection equipment, optical character recognition technology, integrated software and communications systems, as well as training and maintenance to support the host and U.S. Government officials at the SFI ports.

So what have we learned from the SFI work and where do we go from here?

I believe that the SFI pilots have demonstrated that 100 percent scanning of U.S.-bound containers is possible, albeit on a limited scale. For example, we have been able to integrate the radiation scanning equipment with the nonintrusive imaging equipment provided by CBP, thus providing a more powerful tool for detecting shielded nuclear materials by allowing us to look for anomalies in the container, as well as for a radiation alarm. We have been able to transmit large amounts of data on U.S.-bound containers to the local CSI representatives and to CBP in the U.S. for analysis and have provided this and other data to the host governments. We also used the pilot effort in Southampton in the U.K. to demonstrate the usefulness of an advanced spectroscopic portal as a secondary inspection tool. All of this has been accomplished without seriously impacting port operations.

Nonetheless, certain key challenges have been identified through the pilot port effort. From a technology and operational perspective, the most fundamental challenge is to find a way to capture transshipped cargo without seriously impacting port operations. Since transshipped containers do not pass through any entry or exit gate, there is no clear choke point at which the radiation portal monitors and the imaging equipment can be deployed. The operators of large transshipment ports have been consistent in pointing out the operational difficulty of scanning such cargo.

In an attempt to overcome this hurdle, we have been working on several innovative approaches to scan transshipped cargo through the use of straddle carriers as mobile radiation detection devices, and working with CBP and DNDO, on an investigation of crane-mounted detectors. While we are not there yet and the testing continues, some of these technologies appear to hold promise. I would point out, though, that while a solution to transshipped containers may be in the works for radiation detection, it is unclear if such solutions are applicable for the imaging component of SFI in the near term.

The second obvious challenge is cost. Even if the technology is developed to effectively scan 100 percent of the U.S.-bound containers with both imaging and detection systems, it may not nec-

essarily be a cost-effective risk management strategy to equip the 700-plus ports that ship directly to the United States. To maximize our efforts to successfully combat nuclear terrorism, we believe we must strive for an effective layered strategy that addresses multiple threats and risks. We cannot neglect our other priority areas of concern, for example, the First Line of Defense, by putting all of our resources into the latter, into the Second Line of Defense.

In an attempt to address this issue, we have developed cost-sharing arrangements with several SLD and Megaports host partner nations. We also are discussing various models with private industry and encouraging them to integrate scanning into their future port operations. We intend to work closely with CBP and the State Department to promote a risk-based approach to guide implementation priorities.

Another challenge identified through the pilot port effort concerns data sharing. One of our lessons learned has been the difficulty of overcoming laws that prohibit such sharing of information or, alternatively, the lack of a legal framework that will allow us to negotiate such data sharing. These issues must be addressed on a case-by-case basis as they are a point of sensitivity with our partners.

This leads, of course, to the final challenge and that is the need to ensure host nation and terminal operator buy-in. None of these programs overseas will be successful without their direct support.

In summary, the concept of scanning 100 percent of U.S.-bound—

Senator LAUTENBERG. Please conclude as—

Mr. HUIZENGA.—containers overseas has proven to be viable in some ports, and we believe that in light of the lessons learned, a balanced risk-based approach to the deployment of the systems is the best use of available resources.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Huizenga follows:]

PREPARED STATEMENT OF DAVID HUIZENGA, ASSISTANT DEPUTY ADMINISTRATOR,
OFFICE OF INTERNATIONAL MATERIAL PROTECTION AND COOPERATION, DEFENSE
NUCLEAR NONPROLIFERATION, NATIONAL NUCLEAR SECURITY ADMINISTRATION,
U.S. DEPARTMENT OF ENERGY

Introduction

Thank you Chairman Lautenberg, Ranking Member Smith, and other distinguished Members of the Subcommittee. I am the Assistant Deputy Administrator for the Department of Energy—(DOE) National Nuclear Security Administration's (NNSA) Office of International Material Protection and Cooperation (IMPC). My office is one of six program offices within the Office of Defense Nuclear Nonproliferation (DNN). The collective mission of DNN is to detect, prevent, and reverse the proliferation of weapons of mass destruction. Our programs are structured in support of multiple layers of defense against nuclear terrorism and state-sponsored nuclear proliferation. This multi-layered approach is intended to identify and address potential vulnerabilities within the international nonproliferation regime, to limit terrorists' access to deadly weapons and material, and to prevent the illicit trafficking of dangerous materials that could be used in a nuclear or radiological weapon.

Today, I will be discussing NNSA's Megaports Initiative and our role in the Secure Freight Initiative (SFI). I would like to highlight recent progress made under SFI and Megaports. I will also address some of the positive lessons learned from the SFI Pilot deployments and key hurdles that we will have to overcome in order to accelerate and expand the radiation scanning of U.S.-bound containers at foreign seaports as required by the Safe Port and 9/11 Implementation Acts. In short, building on decades of experience securing nuclear materials in DOE's nuclear weapons

complex, NNSA is supplying radiation detection equipment and relevant training to the SFI ports to scan containers for the presence of nuclear and other radioactive materials that could be used by terrorists to fabricate a nuclear or radiological dispersal device.

In summary, we have learned a lot from SFI pilot implementation. The SFI deployments in Honduras, the United Kingdom, and Pakistan indicate that scanning U.S.-bound maritime containers is possible on a limited scale. We have proven that we can effectively integrate data from radiation detection equipment and non-intrusive imaging equipment to improve our overall detection capability, and that we can take this large amount of data and transmit it near real-time to the United States for analysis. While we have been successful at these three locations, transshipment continues to present the greatest challenge to fully implementing the 100 percent scanning requirements. It is clear that obtaining buy-in from the foreign governments and key stakeholders at the port is critical to success. Overall, the concept of scanning U.S.-bound containers overseas has proven to be viable in some cases, but we continue to believe that a risk-based approach to deployment of these systems is the best use of available resources.

We know that the threat of nuclear terrorism is real. It is common knowledge that AlQa'ida's desire to develop weapons of mass destruction goes back at least 10 years. But we also know that ongoing nuclear detection efforts have successfully resulted in seizures of nuclear and radiological materials—underscoring the importance of the nuclear detection mission. For example, in 2003, Georgian border guards, using U.S.-provided portal monitoring equipment at the Sadakhlo border crossing with Armenia, detected and seized approximately 173 grams of highly enriched uranium (HEU) carried by an Armenian national. Also, in late 2005, a Megaports radiation portal monitor (RPM) picked up a neutron signal from a scrap metal container leaving Sri Lanka bound for India. The source of the signal turned out to be an extremely small commercial neutron source, which was found by the Indian authorities. More recently, in November 2007, several Cesium-137 sources were detected in a container of scrap metal leaving Honduras bound for a smelting facility in the Far East. An NNSA team assisted the Honduran Government with the recovery of the industrial sources, preventing those sources from reaching, and possibly contaminating, the facility. These examples provide clear evidence that detection systems are effective in alerting us to the presence of very small quantities of radioactive material and therefore play an important role in our efforts to combat the threat of nuclear terrorism.

Overview of the Material Protection Effort

For the last 15 years, the IMPC office has focused on securing nuclear materials and weapons at well over 100 research, storage and manufacturing facilities in Russia and other states of the Former Soviet Union. Our longstanding nonproliferation programs in international safeguards and export controls have existed for more than 30 years, but the dramatic increase in our efforts to secure nuclear material took place in the years following the demise of the Soviet Union. All of our efforts are centered on the premise that confronting the threat of nuclear terrorism as close to the source as possible, far from our borders, is the most effective means to reduce the risk of an attack. This focus on securing nuclear weapons and materials in-place is the *first line of defense* in our strategy to deny terrorists access to the essential element of a nuclear weapon—fissile material. We are scheduled to complete the vast majority of the nuclear security upgrades at these facilities by the end of 2008 as part of the Bratislava Agreement between President George W. Bush and then-Russian President Vladimir Putin.

Second Line of Defense (SLD) Program

The *Second Line of Defense* (SLD) Program—the other mission area of my office—is a natural complement to these activities and supports the multi-layered defense system to protect the U.S. homeland from attack by a nuclear or radiological dispersal device. The mission of the SLD program is to strengthen the capability of foreign governments to deter, detect, and interdict illicit trafficking in nuclear and other radioactive materials across international borders and through the global maritime shipping system. Under this program, NNSA works collaboratively with foreign partners to equip border crossings, airports and seaports with radiation detection equipment. SLD provides training in the use of the systems for appropriate law enforcement officials and initial system sustainability support while the host government assumes long-term responsibility for the system's operations and maintenance. To date, under the SLD Program, NNSA has installed over 1,000 radiation portal monitors (RPMs) at over 160 sites. The SLD Program has recently awarded contracts to three teams at a value of up to \$700 million for the equipment, design,

integration, and construction expertise to support the deployment of systems in additional locations. The SLD program is divided into two areas: the *Core Program* and the *Megaports Initiative*.

Under our *Core Program*, NNSA focuses primarily on partnerships in Russia, former Soviet states, and Eastern Europe to install radiation detection systems at land borders, international airports, and strategic feeder ports. The SLD Core Program started in 1998 in Russia. Since its inception, the Core Program has worked closely with the Federal Customs Service of the Russian Federation to deploy radiation detection systems to international crossing points throughout Russia. With our Russian colleagues, we have committed to equip all border crossings in Russia (approximately 350 sites) by 2011. Russian Customs is a full partner in this effort and is paying to equip approximately half of these sites themselves. In addition, they will be assuming responsibility for the maintenance of all equipment deployed under this program by 2013.

Megaports Initiative

Building on the experience we have gained by equipping 20 seaports in Russia under the SLD Core Program, in 2003 we expanded the scope of the program to consider large seaports worldwide with the establishment of the Megaports Initiative. This effort was developed in response to the concern that terrorists and states of concern might use the global maritime shipping network to smuggle nuclear or other radioactive materials to locations where terrorists could utilize those materials to fabricate or detonate a nuclear weapon or radiological dispersal device. The goal of the Megaports Initiative is to scan as much container traffic at a port as possible (including imports, exports, and transshipments) regardless of destination.

We began with a focus on the first 20 seaports in the Department of Homeland Security's Container Security Initiative (CSI), *i.e.*, the ports shipping the largest volumes of containerized cargo to the United States. Supported by consultations with the Intelligence Community, private-sector specialists, and our national laboratories, we later added a threat component to our prioritization strategy. As a result, we identified approximately 75 ports of interest (*i.e.*, a little over 10 percent of the total number of container ports shipping directly to the United States) for the deployment of our systems. We update this list periodically based on new information.

I am pleased to report that we have made significant progress on the Megaports Initiative over the last 5 years. We are currently operational in 12 ports (including the three ports selected as pilots under the Department of Homeland Security's Secure Freight Initiative and as mandated by the 2006 SAFE Port Act). We are at various phases of implementation and testing in 27 additional ports. We expect to complete eleven of these ports by the end of this Fiscal Year. We are finalizing agreements with a number of additional countries and continue to conduct outreach and planning activities with approximately 30 other major international seaports in anticipation of implementation in the future. Our goal is to equip approximately 75 priority ports by 2013, at which point we estimate that we will be scanning over 50 percent of global shipping traffic.

Support to Secure Freight Initiative

NNSA has been partnering with the Department of Homeland Security's Customs and Border Protection (CBP) for several years on its container security initiatives. The synergy between the Megaports Initiative and the Container Security Initiative (CSI) is an important element in ensuring the security of U.S.-bound containers—radiation detection equipment provided by NNSA under the Megaports Initiative provides an additional tool that enhances risk assessment and targeting activities at foreign seaports in support of CSI. NNSA has participated with CBP on joint outreach missions and has signed seven agreements jointly with CBP and our international partners to implement both Megaports and CSI. Because of the success of the Megaports Initiative and our ongoing relationship with CBP, partnering on the Secure Freight Initiative (SFI) mission was a natural fit.

In support of SFI, NNSA has provided radiation detection equipment, and associated optical character recognition (OCR) technology, integrated software and communications systems, as well as training and maintenance support, to host and U.S. Government officials at SFI ports. SFI builds upon existing port security measures by utilizing the OCR technology to integrate data from radiation detection and non-intrusive imaging equipment, along with data from secondary inspection equipment, thereby providing more comprehensive information about U.S.-bound containers that strengthens existing risk assessment efforts.

SFI Pilot Lessons Learned and Challenges to 100% Scanning

Let me start by stating that the SFI pilots have demonstrated that 100 percent scanning of U.S.-bound containers is possible on a limited scale. Operationally, we

have been able to demonstrate three different approaches to integrated scanning of the U.S.-bound containers at overseas ports that provide valuable lessons learned as we look to expand scanning efforts to additional ports. We were able to demonstrate both the feasibility of transmitting large amounts of data in near-real time for review and analysis by CBP and the host nation, and the successful integration of multiple sets of data by electronically linking container ID number to scanning data through use of OCR technology. Coupling radiation scans with imaging efforts increases our chances of detecting shielded HEU, because the image allows us to look for anomalies within the contents of the shipping container that might indicate shielding and therefore warrant further inspection. Under SFI, we have demonstrated that these two technologies can be integrated effectively without negatively impacting the flow of commerce, albeit at relatively small ports. We were also able to take advantage of the SFI pilot project in Southampton England, to demonstrate the use of an advanced spectroscopic portal (ASP) as a secondary inspection tool that should dramatically improve the secondary inspection process in terms of reliability, process time, and manpower requirements. Based on lessons learned and the results of the pilot in Southampton, we plan to deploy ASPs to additional Megaports around the world for use in secondary inspections.

Additionally, our partnership with CBP on SFI implementation has been successful and the roles and responsibilities have been well defined. As we have done in our cooperation with CBP for the last several years, we continue to explore ways to maximize use of NNSA and CBP resources, in order to streamline SFI implementation and avoid duplication of efforts.

Nonetheless, in addition to the positive lessons learned from the SFI pilot ports, there are still several challenges to implementing 100 percent scanning of all U.S.-bound containers at overseas ports. We believe that scanning U.S.-bound containers overseas is possible at some locations; however, scanning every U.S.-bound container at a foreign port before it arrives in the United States presents significant operational, technical, cost, and diplomatic challenges. There are a few challenges, in particular, that I would like to focus on as these have the most direct impact on NNSA and the Megaports Initiative.

Transshipment

First, while the operational Megaports and the SFI pilot ports have shown that gate traffic can be easily captured by taking advantage of existing chokepoints into and out of a port, transshipped cargo continues to present a significant challenge for both SFI and Megaports implementation. Because of shorter dwell times for containers, space constraints, availability of shipping data, and the difficulty of identifying chokepoints within the container terminals, capturing transshipments without seriously impacting port operations requires new and creative solutions.

From a technical standpoint, NNSA has been innovative in its approach to scanning transshipped containers. The first mobile detection platform, a straddle carrier, was deployed at the Port of Freeport in the Bahamas in June 2006 using both plastic Polyvinyl Toluene (PVT) for primary detection and a spectroscopic detector for secondary isotopic identification. NNSA, working in conjunction with the terminal operator, Hutchison Port Holdings, has successfully scanned over 730,000 containers at Freeport Container Terminal. We will soon be issuing a request for proposals to provide straddle carriers equipped with radiation detectors at additional transshipment ports.

NNSA is also evaluating a new mobile platform for scanning transshipped containers on the quay at the Port of Salalah, Oman. The mobile system will increase the number of transshipped containers that can be scanned as well as improve the effectiveness and efficiency of the scanning process of transshipped containers with the same efficiency as fixed monitors. Containers will be scanned using the Mobile Radiation Detection and Identification System (MRDIS)—utilizing a plastic PVT for primary detection and a second MRDIS unit with spectroscopic detectors for secondary isotopic identification.

NNSA is currently analyzing crane-based technology, which, if proven effective for the radiation detection component, would improve our ability to scan transshipped containers. In this regard, we are working closely with our colleagues at CBP and at the Domestic Nuclear Detection Office (DNDO) in evaluating private-sector efforts to develop a crane-based radiation detection system utilizing existing spreader-bar technology. We recently conducted a suite of tests on a spreader-bar in the Port of Oakland, California, and will be participating in CBP's upcoming evaluation of spreader-bar systems at their test bed at the Port of Tacoma, WA. We anticipate conducting additional testing and analysis on the effectiveness of these systems at one of our national laboratories later this summer.

While we are hopeful that these technologies will help address the transshipment issue for radiation scanning, it is currently unclear if it would be possible to pursue similar technological solutions to conduct the complementary non-intrusive imaging (NII) scan. In the near term, coupling radiation scans with NII operations at transshipment ports is likely to continue to pose significant technological and operational challenges.

Cost

Moving beyond operational and technical challenges, there is also a significant cost to scanning all U.S.-bound containers before they reach the homeland. Even if technology is developed to effectively scan 100 percent of U.S.-bound containers with both the detection and imaging systems without impacting port operations, it may not necessarily be a cost-effective risk management strategy to equip the 700+ ports that ship directly to the United States. As I mentioned earlier, Megaports and SFI are two programs that support a multi-layered approach to increasing our security against nuclear and radiological threats and defending the homeland from terrorist attacks. We need to ensure that we continue to expand nuclear detection and container security efforts overseas without neglecting other areas of concern that potentially pose greater risk and vulnerability to the country. For example, NNSA also has a responsibility to apply resources and efforts to broader nonproliferation programs including our international material protection program—securing materials at the source—and the SLD Core Program. We must strive for an effective layered strategy that addresses multiple threats and risks in order to reduce the likelihood that dangerous materials will fall into the hands of terrorists. NNSA will continue to promote the use of a risk-based approach to guide implementation priorities to scanning U.S.-bound containers. We will work closely with our interagency partners to prioritize countries and ports as we move ahead with the Megaports Initiative and implementation of SFI, as this approach allows us to utilize our resources and funding in the most effective way.

One obvious way to address the cost of overseas scanning is to encourage cost-sharing with host governments and with private industry. Indeed under the Megaports program, we are finding ways to do this where we provide equipment and training and the host government is responsible for design, construction and installation costs. We are also discussing various models with industry and encouraging them to integrate scanning into their fundamental port operations. Beyond purchasing and installing radiation detection equipment, an integrated scanning system requires effective staffing levels to assess and respond to radiation alarms and image anomalies. Our host nation partners (both government and private sector) will also have to absorb costs associated with increased staffing levels including overtime, training, and personnel assigned to full-time operations.

Data Sharing

Our partnership with the host government also relies on the exchange of information, including scan and image data. One of the lessons learned during the SFI pilot phase is that for some countries, the data sharing requirement presents a significant challenge, either because there are specific laws that prohibit or limit the provision of this type of information or because there is no existing legal framework to allow it to happen. These concerns, along with the issue of reciprocal provision of information on cargo leaving the U.S., will need to be addressed if we continue to expand SFI.

Information exchange is also an important element of the Megaports Initiative. Under Megaports, we have been able to address this issue by limiting the information we receive to data on detections and seizures and by developing specific data-sharing formats; however, it is important to note that data under Megaports is not received in real-time. It is provided to CSI if in-country and to the Embassy.

Stakeholder Partnerships

Which brings me to the last point . . . a critical aspect to implementation of scanning initiatives is host nation and terminal operator buy-in. I cannot underscore enough that SFI or Megaports Initiative implementation cannot be successful without the partnership of the host nation, port authority, terminal operators, and other key stakeholders at the port. We have been very successful where we have strong partnership with our host nation partners. Alternatively, we have had considerable implementation challenges where we have not. For that reason, we will continue to partner with CBP to conduct joint outreach missions in attempt to garner both host government and private-sector support for these critical initiatives. We believe that integrating security measures into the design and business practices of the supply chain will improve security with the least amount of disruption to legitimate trade and could ultimately reduce costs through increased efficiencies. NNSA will con-

tinue to work closely with DHS, host nations, and the major marine terminal operators to develop and implement strategies for increasing container security without impacting port operations.

All in all, the lessons learned during Phase I of SFI implementation have provided us with useful information on how to move ahead with our nuclear detection efforts in the future. However, there are many hurdles and significant costs associated with 100 percent scanning of U.S.-bound containers that need to be carefully considered as we move forward with the SFI program.

Conclusion

In summary, NNSA is committed to continue to expand our Megaports program to scan overseas containers independent of destination and partner with CBP in the SFI efforts to scan U.S.-bound containers. As we consider the expansion of SFI, I believe that NNSA and CBP should continue to work together to identify the ports at which we would like to work by applying the principles of risk-based prioritization, which include both volume and regional threat. We have both utilized such approaches successfully in the past.

We will also continue to work with DHS and the private sector to explore new concepts of operation that will enable us to scan more containers and to investigate new technologies to scan transshipped containers without impacting port operations. We will continue to advocate with the major marine terminal operators that partnering with NNSA and DHS on these container security initiatives makes good business sense.

Finally, while NNSA will continue to support SFI implementation, the Megaports mission has proven to be an important element of our multi-layered defense strategy both from a nonproliferation and counter-terrorism perspective. Indeed, the program is already operational in 12 ports around the world and several more ports should go operational this year. NNSA will continue to push forward with the Megaports Initiative to meet our goal of 75 Megaports by 2013.

I want to thank Congress for their continued support of our program. I hope that the information that I have provided will be useful to the Subcommittee as it considers the SFI pilot project and the future of SFI implementation.

Thank you. I would be happy to answer any questions you may have.

Senator LAUTENBERG. Thank you very much.
Mr. Caldwell?

STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Mr. CALDWELL. Thank you very much, Chairman Lautenberg, for inviting me here to testify on our supply chain security work.

My statement is based on about 5 years' worth of work that GAO has done on supply chain security. Through that time, we have noted that DHS has made progress in a number of ways in developing these programs as part of its layered security strategy to prevent WMD from entering the United States through containers.

As part of this layered strategy, CBP's risk-based approach included two facets, one using shipment information to detect anomalies that might indicate that a container is a high-risk container and only then applying the additional scrutiny of scanning such high-risk containers. This risk-based approach was an attempt to balance the need to improve security while also facilitating the free flow of trade.

CBP's strategy also pushed out the borders through various partnerships. These partnerships were bilateral in the sense that we work with other countries through CSI. They are multilateral in the fact that we work through multilateral organizations such as the World Customs Organization, and there are also private sector partnerships such as the C-TPAT program. I think we all recog-

nize that the private sector actually runs most of the port infrastructure.

And we have reported positively on many of the outcomes of these partnerships. There is good working relationships in many of the CSI ports between the U.S. and the host nation. There is a movement toward, if not the achievement yet, of an international standardized approach to supply chain security through the World Customs Organization's SAFE framework. And finally, there is the industry adoption of improved security standards.

Now, to make these partnerships work, an important part of that was the shared resource burden. It was shared in terms of CSI which was a program where we actually had U.S. staff out at these locations at these ports, but the host nation supplied their own equipment, as well as their own staff to help assist us in targeting and inspecting containers.

The current approach to SFI that CBP has taken, shares some of the characteristics that I have already talked about. In terms of risk management, part of the SFI program is the 10 plus 2 secure filing, and this has been developed as part of the risk-based strategy to plug some of the holes in information that currently exist in the 24-hour rule.

In terms of partnerships, the 10 plus 2 program has also been developed in partnership with industry and international organizations, and similarly the SFI pilot program has been developed with partnerships in the sense that CBP found volunteer ports in countries that were willing to participate.

In terms of resources, again there was some sharing of the resource burden. The U.S. Government supplied the equipment generally, whether it was DOE or CBP. The U.S. Government supplied some of our own staff, over there. But those countries and the port operators, we have to recognize, also supplied a substantial amount of resources as well.

But the ultimate purpose of the SFI pilot was not to continue this layered strategy as much as to test the options of going in a different direction, 100 percent scanning. And now CBP awkwardly finds itself at a crossroad trying to maintain its existing risk-based strategy at the same time Congress is asking it, in some ways, to go in the opposite direction.

Most of the observers believe that the 100 percent scanning approach is contrary to risk management in that it applies the same assumption of risk to all containers before any analysis is done of risk levels.

In addition, the 100 percent scanning requirement is also contrary to the partnership approach that has been used so far, and there have been quite a lot of complaints about this from our partners, whether they be international organizations, other countries, or the private sector.

Moreover, unlike some of the resource sharing that has occurred so far, there seems to be an expectation that foreign governments and foreign ports will be picking up all or most of the additional costs associated with this. So not surprisingly, foreign governments are responding that the flow of trade is going to be harmed. They are talking about a reciprocal requirement which would require that the U.S. scan all of its outbound containers. Most observers

within CBP and our own port operators have raised concerns at least to us in terms of the difficulties that would be involved in that.

Similarly, some of the officials in either foreign governments or the private sector question the value of some of the existing U.S. programs like CSI and C-TPAT. If everything is going to be scanned, they ask what is the point of the risk-based system?

Given that the 100 percent requirement is in our view a marked departure from the existing strategy, we advise to proceed with caution here. CBP needs to continue thoroughly evaluating the SFI program, laying out all the potential challenges and potential ways to overcome those challenges.

And now that the CBP report to Congress is out, we at GAO will start working with your staff, as well as other Committees, to review that program in detail and provide additional information on the way ahead.

Thank you. I would be pleased to answer any questions.

[The prepared statement of Mr. Caldwell follows:]

PREPARED STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY
AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss challenges to 100 percent scanning of U.S.-bound cargo containers. More than 700 foreign seaports ship cargo containers to the United States and over 11 million oceangoing cargo containers arrived at U.S. seaports last year. The terrorist attacks of 2001 heightened concerns about the potential vulnerability of U.S.-bound cargo containers to terrorist exploitation, and the prevention of such activity became a goal for the Federal Government.

Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for preventing terrorists and weapons of mass destruction (WMD) from entering the United States, including the potential WMD threat posed by the movement of oceangoing cargo containers. As it performs this mission, CBP maintains two overarching and sometimes conflicting goals—increasing security while facilitating legitimate trade. To address these goals, CBP has developed a layered security strategy that includes the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). The CSI program, begun in 2002, aims to deter and detect the smuggling of WMD via cargo containers before they reach U.S. seaports. At the 58 seaports participating in the CSI program as of January 2008, foreign governments allow CBP personnel to be stationed at the seaports and use intelligence and automated risk assessment information to determine whether U.S.-bound shipments are at risk of containing WMD or other terrorist contraband—a process referred to as targeting. CBP personnel can then request that host government customs officials scan the identified high-risk cargo.¹ CBP also operates C-TPAT, a voluntary partnership with the trade community, in which member companies commit to improving the security of their supply chains and develop security profiles that outline the companies' security measures. Because of their cooperation, and after verification by CBP that such stronger measures are in place, C-TPAT members generally are subjected to reduced levels of CBP scrutiny of their shipments.

To further address container security concerns, Congress passed, and the President signed, the Security and Accountability for Every (SAFE) Port Act in October 2006, which includes provisions that codified CSI and C-TPAT, both of which had been CBP initiatives but not previously required by law.² In addition, the act calls for the establishment of a pilot program to test the feasibility of scanning 100 percent of U.S.-bound cargo containers and directs CBP to require transmission of additional data from importers and cargo carriers for improved targeting of U.S.-bound cargo containers. CBP is implementing these requirements as part of its Secure

¹ Examining cargo containers involves using radiation detection equipment or nonintrusive imaging equipment, which may include X-ray or gamma ray technology, or both, to determine if a cargo container poses a WMD risk.

² Pub. L. No. 109-347, 120 Stat. 1884.

Freight Initiative (SFI) program. The SAFE Port Act also requires that 100 percent of U.S.-bound cargo containers be scanned using nonintrusive imaging equipment and radiation detection equipment at foreign seaports as soon as feasible. The SFI pilot program tests the feasibility of using this equipment and implementing 100 percent scanning at seven foreign seaports. In August 2007, the Implementing Recommendations of the 9/11 Commission Act (9/11 Act) was enacted, which revised the SAFE Port Act provision on 100 percent scanning to require implementation by 2012, with possible exceptions for seaports for which DHS certifies that specified conditions exist.³

We have issued several reports over the past few years relating to cargo container security that include challenges that are also applicable to 100 percent scanning because of the similarities in the operations of the programs reviewed and their overall purpose to strengthen cargo security.⁴ This statement discusses these and other challenges that relate to the continuation of the SFI pilot program and the longer-term requirement to scan 100 percent of all cargo containers bound for the United States.

The information in this testimony is based on GAO reports and testimonies issued from July 2003 through April 2008 addressing cargo container security operations and programs, as well as ongoing work concerning CBP's international efforts for the Senate Committee on Commerce, Science, and Transportation; the Senate Committee on Homeland Security and Governmental Affairs and its Permanent Subcommittee on Investigations; and the House Committee on Energy and Commerce, to be published later this year. For this ongoing work, we reviewed CBP documents, such as the report on the SFI program required by the 2006 DHS Appropriations Act.⁵ We also reviewed documentation from the World Customs Organization (WCO) related to international initiatives for enhancing supply chain security.⁶ We also analyzed documents from some of CBP's international partners, which include European Commission comments on the SFI Pilot Seaport at Southampton, United Kingdom (UK); a position paper from the Association of German Port Operators; and reports on 100 percent scanning issued by the World Shipping Council and the WCO. In addition, we reviewed available documentation, such as reports and international agreements, related to CBP's work in the international trade community. We also met in Washington, D.C., with CBP officials who have program responsibilities for international affairs and trade, as well as with representatives from the European Commission, the WCO, and industry representative groups to discuss multilateral and bilateral efforts to promote security of the supply chain—the flow of goods from manufacturer to retailer. We also visited six CSI seaports located overseas to meet with local customs officials, selecting the locations based on geographic and strategic significance, container volume to the United States, the dates when the seaports began conducting CSI operations. Although the perspectives of the officials we spoke with cannot be generalized across the wider population of countries that participate in the CSI or C-TPAT programs or that ship container cargo to the United States, they provided us with an overall understanding of how CSI operations were conducted, as well as views on scanning 100 percent of U.S.-bound cargo containers.

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

Summary

In our previous and ongoing work on maritime container security issues, we have identified numerous challenges related to the continuation of the SFI pilot and the longer-term requirement to scan 100 percent of all cargo containers bound for the United States. These challenges are in the following nine areas:

- *Workforce planning:* Given the additional scanning equipment used—as well as the additional cargo containers to be scanned—the SFI pilot, as well as 100 percent scanning, program could generate an increased quantity of scan data. Therefore, CBP could face even greater staffing challenges because more CBP

³Pub. L. No. 110-53, § 1701(a), 121, Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)).

⁴See the end of this statement for a list of related GAO products.

⁵In addition to this report, the SAFE Port Act also required that CBP produce a report on lessons learned from the SFI pilot program; however, this report was not available as of the time we prepared this statement.

⁶The WCO is an independent international organization whose mission is to enhance the efficiency and effectiveness of customs administrations.

officers will be required to review and analyze these data for participating seaports. Furthermore, our past work on maritime container security found weaknesses in CBP's workforce planning.

- *Host nation examination practices:* While the SAFE Port and 9/11 Acts require DHS to develop operational and equipment standards for the scanning systems used for 100 percent scanning, CBP does not systematically collect information on the efficacy of host government examination systems.
- *Measuring performance:* While the intention of the SFI pilot program and 100 percent scanning is to increase security for the United States, CBP has had ongoing difficulties in defining performance measures for its maritime container security programs to indicate whether security is increased.
- *Resource responsibilities:* It is unclear who will pay for additional resources—including increased staff, equipment, and infrastructure—and who will be responsible for operating and maintaining the equipment used for the statutory requirement to scan 100 percent of U.S.-bound cargo containers at foreign seaports. Neither the SAFE Port Act nor the 9/11 Act specifies whether the Federal Government will bear the cost of scanning 100 percent of U.S.-bound cargo containers.
- *Logistics:* Scanning equipment is sometimes placed miles from where cargo containers are stored, which could add to the time and cost requirements for scanning these containers, and transshipment cargo containers—containers moved from one vessel to another—are only available for scanning for a comparatively short period of time and may be difficult to access.
- *Technology and infrastructure:* Issues, such as environmental conditions that damage equipment and cause delay, limited bandwidth capacity of local infrastructure, and compatibility with older equipment have presented difficulties in the SFI pilot program.
- *Use and ownership of data:* While the SAFE Port Act specifies that scan data produced in the SFI pilot program should be available for review by U.S. officials, legal restrictions in foreign countries may make it difficult to share this information with CBP. In some cases, transferring such information to U.S. officials could require new international agreements.
- *Consistency with risk management:* International partners state that 100 percent scanning is inconsistent with widely accepted risk management principles, and some CBP international partners have stated that the requirement could potentially reduce the security of the supply chain by diverting scarce resources away from other essential security measures.
- *Reciprocity and trade concerns:* Foreign governments could call for reciprocity of 100 percent scanning, requiring the United States to scan container exports to those countries. This will be a challenge, as CBP officials have stated that the agency does not have the resources to scan other countries' exports leaving the United States. Further, some view this scanning requirement as a barrier to trade.

Background

CBP Has Developed a Layered Security Strategy to Help Implement Its Risk Management Approach

CBP has developed a layered security strategy that provides multiple opportunities to mitigate threats and allows CBP to focus its limited resources on cargo containers that are the most likely to pose a risk to the United States. Risk management is a strategy called for by Federal law and Presidential directive and is meant to help policymakers and program officials most effectively mitigate risk while allocating limited resources under conditions of uncertainty. This layered security strategy is composed of different but complementary initiatives and programs, such as CSI and C-TPAT, which build on each other and work with other Federal security programs, such as the Department of Energy's (DOE) Megaports Initiative.⁷ This layered strategy attempts to address cargo container security comprehensively while ensuring that security attention is directed toward the highest-risk containers within the supply chain.

⁷Begun in 2003, DOE's Megaports Initiative complements CBP's layered security strategy by providing foreign nations with radiation detection equipment, such as radiation portal monitors, to scan cargo containers moving through their seaports. As of February 2008, the Megaports Initiative was fully operational at 12 foreign seaports and in various stages of implementation at 17 others.

The Container Security Initiative

CBP's CSI program aims to identify and examine U.S.-bound cargo that pose a high risk of concealing WMD or other terrorist contraband by reviewing advanced cargo information sent by ocean cargo carriers. As of January 2008, CBP operated CSI in 58 foreign seaports, which, at the time, accounted for 86 percent of all U.S.-bound cargo containers. As part of the CSI program, CBP officers, usually stationed at foreign seaports, seek to identify high-risk U.S.-bound cargo containers by using information from cargo carriers as well as reviewing data bases and interacting with host government officials. When requested by CBP, host government customs officials examine the high-risk container cargo by scanning it using various types of nonintrusive inspection (NII) equipment, such as large-scale X-ray machines, or by physically searching a container's contents before it is sent to the United States.⁸

Customs-Trade Partnership against Terrorism

Initiated in November 2001, the C-TPAT program aims to secure the flow of goods bound for the United States by developing a voluntary antiterrorism partnership with stakeholders from the international trade community.⁹ To join C-TPAT, a company submits a security profile, which CBP compares to its minimum security requirements for the company's trade sector. CBP then reviews the company's compliance with customs laws and regulations and any violation history that might preclude the approval of benefits—which includes reduced scrutiny or expedited processing of the company's shipments. CBP data show that from 2004 through 2006, C-TPAT members were responsible for importing about 30 percent of U.S.-bound cargo containers, specifically importing 29.5 percent of the 11.7 million oceangoing cargo containers off-loaded in the United States in the first 9 months of 2007. As of May 2008, there were over 8,400 C-TPAT members from the import trade community that had various roles in the supply chain.

The Importance of International Partnerships

To more effectively implement the components of its layered security strategy, CBP has worked to promote international partnerships to enhance security so that high-risk cargo can be identified before it arrives in the United States. For the CSI program, CBP has negotiated and entered into nonbinding, reciprocal arrangements with foreign governments, specifying the placement of CBP officials at foreign seaports and the exchange of information between CBP and foreign customs administrations. These arrangements allow participating foreign governments the opportunity to place their customs officials at U.S. seaports and request inspection of cargo containers departing from the United States that are bound for their respective countries. CBP also works with other customs organizations to enhance international supply chain security. For example, CBP has taken a lead role in working with foreign customs administrations and the WCO to establish and implement international risk-based management principles and standards, similar to those used in the CSI and C-TPAT programs, to improve the ability of member customs administrations to increase the security of the global supply chain while facilitating international trade. The member countries of the WCO, including the United States, adopted such risk-based principles and standards through the WCO Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework), in June 2005.

The SAFE Port Act Requires a Pilot Program to Test the Feasibility of 100 Percent Scanning

To improve maritime container security, the SAFE Port Act was enacted in October 2006 and requires, among other things, that CBP conduct a pilot program to determine the feasibility of scanning 100 percent of U.S.-bound containers. It also specifies that the pilot should test integrated scanning systems that combine the use of radiation portal monitors and NII equipment, building upon CSI and the Megaports Initiative. To fulfill this and other requirements of the SAFE Port Act, CBP and DOE jointly announced the formation of SFI in December 2006. The first phase of SFI is the International Container Security project—commonly known as

⁸There are generally two types of CSI cargo container examinations—scanning with NII equipment and physical searches. To scan cargo containers, CSI depends on imaging equipment, which may use X-rays or gamma rays to create images of the container's contents, and radiation detection equipment. CBP officials, along with host government officials, may review the information produced with the scanning equipment to determine the presence of WMD. Depending on the results of the scans, physical searches may be conducted.

⁹Stakeholders of the international trade community include importers; customs brokers; air, sea, and land carriers; and other logistics service providers, such as freight consolidators.

the SFI pilot program.¹⁰ The SFI pilot program tests the feasibility of 100 percent scanning of U.S.-bound container cargo at seven overseas seaports and involves the deployment of advanced cargo scanning equipment and an integrated examination system. The advanced cargo scanning equipment—NII and radiation detection equipment—produce data to indicate the presence of illicit nuclear and radiological material in containers. The integrated examination system then uses software to make this information available to CBP for analysis. According to CBP, it will review the scan data at the foreign seaport or at CBP's National Targeting Center-Cargo (NTCC) in the United States.¹¹ If the scanning equipment indicates a potential concern, both CSI and host government customs officials are to simultaneously receive an alert and the specific container is to be further inspected before it continues on to the United States.

As shown in table 1, under the SFI pilot program, three SFI seaports are to scan 100 percent of U.S.-bound container cargo that passes through those seaports, while the other four seaports are to deploy scanning equipment in a more limited capacity.

Table 1.—Information on the Seven Foreign Seaports Participating in the SFI Pilot Program

SFI port	Deployment level when pilot operational	Testing date ^a	Operational date ^b	Volume of U.S.-bound containers, Fiscal Year 2006
Qasim, Pakistan	Full ^c	March 2007	October 12, 2007	2,058
Puerto Cortez, Honduras	Full ^c	April 2007	October 12, 2007	77,707
Southampton, UK	Full ^c	August 2007	October 12, 2007	31,780
Busan, South Korea	Limited ^d	April 2008 (projected)	To be determined	610,061
Salalah, Oman	Limited ^d	May 2008 (projected)	To be determined	81,333
Singapore	Limited ^d	June 2008 (projected)	To be determined	376,846
Hong Kong	Limited ^d	November 2007	January 2008	1,333,812

Source: U.S. Customs and Border Protection.

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

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

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

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

As required by the SAFE Port Act, CBP was to issue a report in April 2008 on the lessons learned from the SFI pilot program and the need and feasibility of expanding the 100 percent scanning system to other CSI seaports, among other things.¹² As we prepared this statement, CBP had not yet issued this report. Every 6 months after the issuance of this report, CBP is to report on the status of full-scale deployment of the integrated scanning systems at foreign seaports to scan 100 percent of U.S.-bound cargo.

The SFI Pilot Program and 100 Percent Scanning Face a Number of Challenges

We identified challenges in nine areas that are related to the continuation of the SFI pilot program and the longer-term 100 percent scanning requirement: (1) workforce planning, (2) the lack of information about host government cargo examination

¹⁰The second phase of SFI is still in development. This phase involves the advance transmission of cargo information from importers and cargo carriers.

¹¹According to CBP, the National Targeting Center (NTC) was established in response to the need for proactive targeting aimed at preventing acts of terror and to seize, deter, and disrupt terrorists and implements of terror. NTC originally combined both passenger and cargo targeting in one facility. It was later divided into NTCC and the National Targeting Center-Passenger. For purposes of this report, we use NTCC in our references since its mission is to support CBP cargo-targeting operations.

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

systems, (3) measuring performance outcomes, (4) undefined resource responsibilities for the cost and labor for implementation, (5) logistical feasibility for scanning equipment and processes, (6) technological issues, (7) the use and ownership of scanning data, (8) a perceived disparity between 100 percent scanning and the risk management approach of CBP's international partners, and (9) potential requests for reciprocity from foreign governments.

Workforce Planning Will Be Critical to Success

In our prior work examining the CSI and C-TPAT programs, we reported that CBP faced challenges identifying an appropriate number of positions for the programs and finding enough qualified people to fill these positions.¹³ For example, we reported in 2005 and again in 2008 that CBP's human capital plan did not systematically determine the optimal number of officers needed at each CSI seaport to carry out duties that require an overseas presence (such as coordinating with host government officials or witnessing the examinations they conduct) as opposed to duties that could be performed remotely in the United States (such as reviewing data bases).¹⁴ Determining optimal staffing levels is particularly important since CBP reports facing ongoing challenges identifying sufficient numbers of qualified employees to staff the program. For example, CBP officials reported that 9 qualified applicants applied for 40 permanent positions at CSI seaports. We also reported that according to CBP officials, to fill open CSI positions, officers have in some cases been deployed who have not received all required training. We recommended in April 2005 that CBP revise the CSI staffing model to consider: (1) what functions need to be performed at CSI seaports and what can be performed in the United States, (2) the optimum levels of staff needed at CSI seaports 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 seaports instead of in the United States.¹⁵ CBP agreed with our recommendation on CSI's staffing model and said that modifications to the model would allow program objectives to be achieved in a more cost-effective manner. CBP said that it would evaluate the minimum level of staff needed at CSI seaports to maintain ongoing dialogue with host nation officials, as well as assess the staffing levels needed domestically to support CSI activities. However, as of January 2008, CBP's human capital plan did not systematically make these determinations.

The ability of the SFI pilot program—and by extension the 100 percent scanning requirement of the SAFE Port and 9/11 Acts—to operate effectively and enhance maritime container security depends, in part, on the success of CBP's ability to manage and deploy staff in a way that ensures that critical security functions are performed. Under the CSI program, CBP operated and conducted cargo container scanning at 58 foreign seaports as of January 2008; however, given that additional scanning equipment will be used in the SFI pilot program, and fulfilling the 100 percent scanning requirement will naturally increase the number of containers to be scanned at the more than 700 seaports that ship cargo to the United States, the SFI pilot program and 100 percent scanning requirement will generate an increased quantity of scan data. According to European customs officials, for there to be value added in these additional scans, the scan data must be reviewed. Therefore, in implementing the 100 percent scanning requirement, CBP will face staffing challenges because more CBP officers will be required to review and analyze these data for participating seaports.

CBP Generally Lacks Key Information on Host Government Examination Systems Because of Sovereignty Constraints

As we reported in January 2008, CBP does not systematically collect information on CSI host governments' examination equipment or processes.¹⁶ We noted that CBP must respect the sovereignty of countries participating in CSI and, therefore, cannot require that a country use specific scanning equipment or follow a set of pre-

¹³For our prior recommendations and observations on C-TPAT's workforce challenges, see 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). Also, see GAO, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 11, 2005).

¹⁴GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO 05 557 (Washington, D.C.: Apr. 26, 2005) and GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, GAO 08 187 (Washington, D.C.: Jan. 25, 2008).

¹⁵GAO-05-557.

¹⁶GAO-08-187.

scribed examination practices. Thus, while CBP has set minimum technical criteria to evaluate the quality and performance of equipment being considered for use at domestic seaports, it has no comparable standards for scanning equipment used at foreign seaports. In addition, CBP officials stated that there are no plans to evaluate examination equipment at foreign seaports against the domestic criteria. CBP officials added, however, that the capabilities of scanning equipment are only one element for determining the effectiveness of examinations that take place at CSI seaports. It is better, in their view, to make assessments of the processes, personnel, and equipment that collectively constitute the host governments' entire examination systems. However, in January 2008, we reported that CBP does not gather this type of information and recommended that CBP, in collaboration with host government officials, improve the information gathered at each CSI port by: (1) establishing general guidelines and technical criteria regarding the minimal capability and operating procedures for an examination system that can provide a basis for determining the reliability of examinations and related CSI activities; (2) systematically collecting data for that purpose; and (3) analyzing the data against the guidelines and technical criteria to determine what, if any, mitigating actions or incentives CBP should take to help ensure the desired level of security. CBP partially concurred with this recommendation in terms of improving the information gathered about host governments' examination systems. In particular, CBP agreed on the importance of an accepted examination process and noted that it continues to improve the information it gathers. CBP did not indicate that it would systematically pursue information on these host government examination systems. It did state that it was working through the WCO to address uniform technical standards for equipment. We reported that while CBP engaged with international trade groups to develop supply chain security requirements, these requirements do not specify particular equipment capabilities or examination practices.

Both the SAFE Port and 9/11 Acts require DHS to develop technical and operational standards for scanning systems; therefore, the challenges that CSI has faced in obtaining information about host governments' examination systems are relevant to the SFI pilot program and the 100 percent scanning requirement.¹⁷ However, as noted earlier in this statement, the United States cannot compel foreign governments to use specific equipment for the SFI pilot program or the 100 percent scanning requirement, thus challenging CBP's ability to set and enforce standards. In addition, because CBP does not systematically collect information on the efficacy of host governments' examinations systems, it lacks reasonable assurance that these examinations could reliably detect and identify WMD unless it implements our January 2008 recommendation to determine actions to take to ensure the desired level of security. This is particularly important since currently, under CSI, most high-risk cargo containers examined at international seaports are not re-examined upon arrival at domestic seaports.

Measuring Performance, Particularly Outcomes, Will Be Difficult

In our reviews of the CSI and C-TPAT programs, we identified challenges with CBP's ability to measure program performance because of, among other things, the difficulty in determining whether these programs were achieving their desired result of increasing security for the United States.¹⁸ In the past, we and the Office of Management and Budget (OMB) have acknowledged the difficulty in developing outcome-based performance measures for programs that aim to deter or prevent specific behaviors.¹⁹ In the case of C-TPAT, we noted in our March 2005²⁰ and April 2008 reports that CBP had not developed a comprehensive set of performance meas-

¹⁷The SAFE Port Act directs DHS to: (1) establish technical criteria and standard operating procedures for the use of NII equipment at CSI seaports and (2) require CSI seaports to operate the equipment in accordance with the criteria and operating procedures established by DHS. The act states that the technical criteria and operating procedures should not be designed to conflict with the sovereignty of host countries, but it did not address host government's sovereignty related to requirements for CSI seaports to operate the equipment in accordance with the criteria and procedures. The 9/11 Act directs DHS to establish technological and operational standards for systems to conduct 100 percent scanning of containers and to ensure that this and other actions taken to implement 100 percent scanning are consistent with the United States' international obligations.

¹⁸For more information on the difficulty that CSI has had in developing outcome-based performance measures and in measuring the deterrence effect of the program, see GAO-08-187.

¹⁹According to OMB, outcome measures describe the intended result of carrying out a program or activity. For example, for a tornado warning system, a measure of outcome could be the number of lives saved and amount of property damage averted.

²⁰GAO-05-404 and GAO, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, GAO-08-240 (Washington, D.C.: Apr. 25, 2008).

ures and indicators for the programs, such as outcome-based measures, to monitor the status of program goals. A senior CBP official stated that developing these measures for C-TPAT, as well as other CBP programs, has been difficult because CBP lacks the data necessary to determine whether a program has prevented or deterred terrorist activity. We recommended that CBP 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. CBP agreed with our recommendation on developing performance measures, and had developed initial measures relating to membership, inspection percentages, and validation effectiveness. However, as we reported in April 2008, CBP had yet to develop measures that assess C-TPAT's progress toward achieving its strategic goal to ensure that its members improve the security of their supply chains pursuant to C-TPAT security criteria.

Given that, as with CSI and C-TPAT, the purpose of the SFI pilot program and the 100 percent scanning provision is to increase security for the United States, the same challenges related to defining and measuring performance could also apply to the SFI pilot program and the 100 percent scanning provision. Without outcome-based performance measures, it will be difficult for CBP and DHS managers and Congress to effectively provide program oversight and determine whether 100 percent scanning achieves the desired result—namely increased security for the United States.

Resource Responsibilities for Implementing 100 Percent Scanning Have Not Been Determined

While CBP and DOE have purchased security equipment for foreign seaports participating in the SFI pilot program, it is unclear who will pay for additional resources—including increased staff, equipment, and infrastructure—and who will be responsible for operating and maintaining the equipment used for the statutory requirement to scan 100 percent of U.S.-bound cargo containers at foreign seaports. According to CBP, the average cost of initiating operations at CSI seaports was about \$395,000 in 2004 and \$227,000 in 2005.²¹ By comparison, CBP reported that it and DOE have spent approximately \$60 million, collectively, to implement 100 percent scanning at the three foreign seaports fully participating in the SFI pilot program.²² The SAFE Port and 9/11 Acts did not require nor prohibit the Federal Government from bearing the cost of scanning 100 percent of U.S.-bound cargo containers.²³ According to customs officials in the U.K. who participated in the SFI pilot program at the Port of Southampton, resource issues will inhibit their ability to implement permanently the 100 percent scanning requirement. For example, these customs officials commented that to accommodate the SFI pilot program at the Port of Southampton, existing customs staff had to be reallocated from other functions. The U.K. customs officials further stated that this reallocation was feasible for the 6-month pilot program, but it would not be feasible on a permanent basis. Similarly, a customs official from another country with whom we met told us that while his country does not scan 100 percent of exports, its customs service has increased its focus on examining more exported container cargo, and this shift has led to a 50 percent increase in personnel.

European government officials expressed concerns regarding the cost of equipment to meet the 100 percent scanning requirement, as well as the cost of additional personnel necessary to operate the new scanning equipment, view and transmit the images to the United States, and resolve false alarms. Though CBP and DOE have provided the bulk of equipment and other infrastructure necessary to implement the SFI pilot program, they have also benefited from host nation officials and port operators willing to provide, to varying degrees, the resources associated with additional staffing, alarm response protocols, construction, and other infrastructure upgrades. However, according to CBP, there is no assurance that this kind of mutual support

²¹ CBP had used the average cost per CSI port to achieve operational status as a performance measure. However, agency officials told us that they stopped using the measure in 2006 because at that point, the majority of CSI seaports had already become operational and because there were too many variables beyond CBP's control in the calculation.

²² Under the SFI pilot program, three seaports will scan 100 percent of U.S.-bound container cargo while the remaining four will scan less than 100 percent of U.S.-bound container cargo. CBP will conduct a reduced level of SFI operations at these four seaports, typically limited to one terminal in the port, such as Gamman Terminal in Busan or the Brani Terminal in Singapore.

²³ However, the Congressional Budget Office assumed in its analysis of estimates for implementing this requirement that the cost of acquiring, installing, and maintaining systems necessary to comply with the 100 percent scanning requirement would be borne by foreign seaports so that they could maintain trade with the United States.

is either sustainable in the long term or exists in all countries or at all seaports that export goods to the United States.

Logistical Feasibility Could Vary by Seaport

Logistical issues, such as crowded terminal facilities and the variety of transportation modes at terminals, could present challenges to the SFI pilot program and implementation of 100 percent scanning. Seaports may lack the space necessary to install additional scanning equipment needed to comply with the 100 percent scanning requirement. For example, we observed that scanning equipment at some seaports is located several miles away from where cargo containers are stored, which could add to the time and cost requirements for scanning these containers. Similarly, while some seaports have natural bottlenecks that allow for container scanning equipment to be placed such that all outgoing containers would have to pass through the equipment, not all seaports are so configured, and the potential exists for containers to be shipped to the United States without being scanned. Another potential logistical vulnerability is related to the transportation modes by which cargo containers arrive and pass through seaports. For example, cargo containers that arrive at a seaport by truck or rail are generally easier to isolate, whereas transshipment cargo containers—those moved from one vessel to another—are only available for scanning for a comparatively short time and may be more difficult to access.²⁴ For example, U.K. customs officials stated that it was not possible to route transshipment containers that arrived by sea through the SFI equipment. As a consequence, according to CBP officials, the scanning of transshipment containers has not begun at the Port of Southampton. CBP and European customs officials evaluating the SFI pilot program stated that while the pilot has been comparatively successful at relatively lower-volume seaports, such as Southampton, implementing 100 percent scanning would be significantly more challenging at seaports with a higher volume of cargo container traffic or greater percentages of transshipment cargo containers.

Technology and Compatibility Issues Could Present Challenges

The SFI pilot program currently faces technology challenges, such as mechanical breakdowns of scanning equipment because of environmental factors, inadequate infrastructure for the transmission of electronic information, and difficulties in integrating different generations of scanning equipment. Environmental conditions at some sites can compromise the effectiveness of radiation detection equipment used in the SFI pilot program. For example, two of the three seaports fully participating in the SFI pilot program experienced weather-related mechanical breakdowns of scanning equipment. Specifically, at the Port of Southampton, a piece of radiation scanning equipment failed because of rainy conditions and had to be replaced, resulting in 2 weeks of diminished scanning capabilities. Additionally, Port Qasim in Pakistan has experienced difficulties with scanning equipment because of the extreme heat. Because of the range of climates at the more than 700 other international seaports that ship cargo to the United States, these types of technological challenges could be experienced elsewhere.

The limited infrastructure at some foreign seaports poses a challenge to the installation and operation of radiation detection equipment, as well as to the electronic transmission of scan data to CBP officers in the United States. Many seaports are located in remote areas that often do not have access to reliable supplies of electricity or infrastructure needed to operate radiation portal monitors and associated communication systems. For example, at Port Salalah in Oman, a key challenge has been the cost of data transmission, because of low bandwidth communications infrastructure, to send data to the CBP officers who review the scans. Prior to SFI, the CSI office in Port Salalah already used transmission technology that cost annually about 10 times that of other SFI seaports. To participate in SFI, CBP originally planned to procure additional technology costing approximately \$1.5 million each year to transmit the SFI data from Port Salalah. However, CBP was able to devise a lower-cost option that involved sharing communications infrastructure with existing CSI operations at the port because U.S.-bound container volume is relatively low in Oman. While CBP reported that this solution could keep data transmission costs down at other low-volume seaports, it is unclear whether this could be accomplished at higher-volume seaports. In addition to compatibility with existing infrastructure, SFI seaports have experienced compatibility issues with equipment from different generations. According to CBP, there are various manufacturers of equipment used at CSI seaports, and although the integration of equipment and technology at SFI

²⁴ Similarly, it may be difficult to scan cargo containers that remain on board a vessel as it passes through a foreign seaport.

pilot program seaports has generally been successful, it has not been without challenges. For example, at Port Salalah integration of a large number of new pieces of equipment by new vendors caused operational delays.

Use and Ownership of Data Have Not Been Determined

The legislation that mandated the SFI pilot program and 100 percent scanning does not specify who will have the authority or responsibility to collect, maintain, disseminate, view, or analyze scan data collected on cargo containers bound for the United States. While the SAFE Port Act specifies that SFI pilot program scan data should be available for review by U.S. Government officials, neither it nor the 9/11 Act establishes who is to be responsible for managing the data collected at foreign seaports. Other unresolved questions include ownership of data, how proprietary information is to be treated, and how privacy concerns are to be addressed. For example, officials from U.K. Customs stated that U.K. privacy legislation barred sharing information on cargo containers with CBP unless a specific risk was associated with the containers. To comply with U.K. laws, while still allowing CBP to obtain scan data on container cargo, U.K. Customs and CBP negotiated working practices to allow CBP to use its own handheld radiation scanning devices to determine whether cargo containers emitted radiation, but this was only for purposes of the SFI pilot program. According to the European Commission, for 100 percent scanning to go forward, the transfer of sensitive information would have to take place systematically, which would only be possible if a new international agreement between the United States and the European Union (EU) was enacted. In the absence of agreements with the host governments at the more than 700 seaports that ship cargo to the United States, access to data on the results of container scans could be difficult to ensure.

CBP International Partners Have Stated That 100 Percent Scanning Is Inconsistent with Widely Accepted Risk Management Practices

Some of CBP's international partners, including foreign customs services, port operators, trade groups, and international organizations, have stated that the 100 percent scanning requirement is inconsistent with widely accepted risk management principles, and some governments have expressed to DHS and Congress that 100 percent scanning is not consistent with these principles as contained in the SAFE Framework.²⁵ Similarly, some European customs officials have told us that the 100 percent scanning requirement is in contrast to the risk-based strategy behind CSI and C-TPAT, and the WCO has stated that implementation of 100 percent scanning would be "tantamount to abandonment of risk management." In addition, some of CBP's international partners have stated that the requirement could potentially reduce security. For example, the European Commission noted that there has been no demonstration that 100 percent scanning is a better means for enhancing security than current risk-based methods. Further, CBP officials have told us that the 100 percent scanning requirement may be a disincentive for foreign countries or companies to adopt risk-based security initiatives, such as CSI, C-TPAT, or the SAFE Framework. Similarly, in April 2008, the Association of German Seaport Operators released a position paper that stated that implementing the 100 percent scanning requirement would undermine mutual, already achieved security successes and hinder maritime security by depriving resources from areas that present a more significant threat and warrant closer scrutiny.

100 Percent Scanning Could Lead to Calls for Reciprocity and Be Viewed as a Barrier to Trade

Implementation of the 100 percent scanning requirement could result in calls for reciprocity of scanning activities from foreign officials and be viewed as a barrier to trade. European customs officials, as well as officials from the WCO, have objected to the unilateral nature of the 100 percent scanning requirement, noting that this requirement contrasts with prior multilateral efforts CBP has implemented. Similarly, the Association of German Port Operators published a position paper stating that the legislative requirement inherently ignores the international character of global maritime trade and is a classic example of an issue that should have been discussed with and passed by the legislative body of an international organization, such as the WCO. In its report on the SFI pilot program, the European Commission expressed concern that it would be difficult for EU customs administrations

²⁵ Currently, the CSI program employs a risk management approach to identify cargo containers at high risk of containing WMD for scanning with nonintrusive imaging equipment and possible physical inspection before being placed on vessels bound for the United States. In contrast, the 100 percent scanning approach subjects to all U.S.-bound cargo containers to scanning with nonintrusive imaging equipment regardless of risk.

to implement a measure designed to protect the United States that would divert resources away from strengthening EU security. Customs officials from Europe, as well as members of the World Shipping Council and the Federation of European Private Port Operators, indicated that should implementation of the 100 percent scanning requirement be pursued, foreign governments could establish similar requirements for the United States, forcing U.S. export cargo containers to undergo scanning before being loaded at U.S. seaports. According to CBP officials, the SFI pilot program, as an extension of CSI, allows foreign officials to ask the United States to reciprocate and scan 100 percent of cargo containers bound for their respective countries. CBP officials told us that CBP does not have the personnel, equipment, or space to scan 100 percent of cargo containers being exported to other countries, should it be requested to do so.

In addition to the issue of reciprocity, European and Asian government officials, as well as officials from the WCO, have stated that 100 percent scanning could constitute a barrier to trade. For example, the Association of German Seaport Operators stated that the 100 percent mandate would amount to an unfair nontariff trade barrier between the United States and foreign seaports. Similarly, senior officials from the European Commission expressed concern that a 100 percent scanning requirement placed on foreign seaports could disrupt the international trading system.²⁶ Further, the WCO passed a unanimous resolution in December 2007, expressing concern that implementation of 100 percent scanning would be detrimental to world trade and could result in unreasonable delays, port congestion, and international trading difficulties.²⁷

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement. We look forward to working with CBP and the Congress to track progress of the SFI pilot and to identify the way forward for supply chain security. I would be happy to respond to any questions you may have.

Related GAO Products

Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices. GAO-08-240. Washington, D.C.: April 25, 2008.

Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed. GAO-08-187. Washington, D.C.: January 25, 2008.

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

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

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

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

Maritime Security: Observations on Selected Aspects of the SAFE Port Act. GAO-07-754T. Washington, D.C.: April 26, 2007.

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

Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System. GAO-06-591T. Washington, D.C.: March 30, 2006.

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

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

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

Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts. GAO-05-557. Washington, D.C.: April 26, 2005.

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

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

²⁶The European Commission is the EU's policy-making and executive engine. The commission is composed of 27 commissioners, one from each member state. Among its many powers, the commission proposes legislation for approval by the EU Council and European Parliament in matters relating to economic integration, ensures that EU laws are applied and upheld throughout the EU, implements the budget, and represents the European community in international trade negotiations.

²⁷The United States abstained from the vote.

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

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

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

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

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

Senator LAUTENBERG. Thank you very much.

I would like a definition, Mr. Caldwell. How would you describe a layered approach to things? Is it basically modular?

Mr. CALDWELL. Well, the layered approach is several different programs trying to get at different parts of vectors that terrorists may use to get a weapon of mass destruction or other kind of contraband into this country. Part of that layer is Megaports that the Department of Energy operates to look for containers that would contain radioactive WMD. CBP's layers include, first, advance information to try to get information which could reveal potential—

Senator LAUTENBERG. But tell me, does that not really describe the whole picture? I think when we modify the design of the program with a layered approach—I do not think that is any different than the approach to get to the end of the game, regardless of route. I mean, you have to do these things. What concerns me is that layered comes in there as an opportunity, Mr. Ahern, for the inability to meet a target that we have for the 100 percent scanning. So we use different words to describe it. “Layered” is one of them.

And I talked to several of the staff as well.

I mean, to me it is which of the routes is most important. Well, you have to consider that totally when you are looking for the security that we would like to see.

Mr. Ahern, the Congress last year passed a law requiring all shipping containers coming into our ports to be scanned for nuclear weapons and radiation before they reach our shores. Now, according to the testimony this morning, the July 2012 deadline will not be met. What will you say is a reasonable expectation now to have a 100 percent scanning system in place for all maritime cargo coming into the United States?

Mr. AHERN. Well, as stated, the 2012 deadline that was actually expressed in the 9/11 Act had six caveats where there could be extensions if certain conditions were not met. Those are very specific in the law: making sure there was sufficient equipment available for purchase and installation; sufficient low false alarm rates; the capability to physically deploy the logistical challenges, some of which I described in some minimal detail, which is much more described in the report, some of the physical lay-down challenges we have seen in two very small ports that we have tested it in; the integration with the existing systems. I mean, Mr. Huizenga spoke about the fact that integrating the systems. Yes, there is a complementary package of technology that is out there, but one of the other conditions is about the software anomaly recognition system.

Senator LAUTENBERG. Yes. Listen, we have got lots of brilliant people who are helping to devise the program into place. Why are all of these things anomalous? To me it seems that is part of what

you do in order to make an estimate. Otherwise, it is kind of hip shooting and picking out a date. From day one almost, it says that we are never going to meet this date.

Mr. AHERN. Let me try to simplify it as best I can. The anomaly recognition, to be able to look at each one of the X-rays that comes through the gates for the containers—if we were to apply that against a universal 11.5 million containers, continuing to grow each year by 10 to 12 percent, it is not a matter of just running the containers through the X-ray systems. At this point in time, someone—that means a human, a trained officer, we believe a Government officer—needs to be able to go ahead and look and review those images. That takes——

Senator LAUTENBERG. You mean that was not thought of?

Mr. AHERN. No. That has absolutely been thought of. We have made this very clear for a number of years——

Senator LAUTENBERG. So why do we not get past the problems that exist and answer the question, well, why in the planning were these things not reviewed? Why were these situations not expected? If it was a NASA flight, it would be terrible if the planning had been this far off the mark.

Mr. AHERN. Well, very respectfully, sir, there is conflicting direction from the Congress. The SAFE Port Act actually was going to give us the opportunity to go ahead and provide the opportunity to study through piloting three locations, which we are underway, in the process of doing, which is the report that was just submitted late.

The 9/11 Act that came along later then just trumped that legislation and basically called for 100 percent scanning of all containers coming into the United States. So there was not the opportunity to continue to work through the pilot in an appropriate fashion to discover all the concerns that are out there with the development and maturity of technology, the integrating of the images, the software anomaly recognition capabilities, the challenges to sovereignty that we have out there as well, and also deal with some of the diplomatic challenges.

One of the things I would like to present to you—and I would really offer it into the record for your consideration for the full committee here—is that we have had 27 countries that have written to us and expressed their concerns. We have had nine international trade associations and two international associations.

[The information referred to follows:]

LIST OF COUNTRIES AND TRADE ORGANIZATIONS EXPRESSING CONCERNS
ON 100 PERCENT SCANNING

Provided by U.S. Customs and Border Protection

Countries:

Australia
Belgium
Bulgaria
Cameroon
Canada
China
Finland
Germany
Honduras
Hong Kong
Indonesia
Italy
Japan
Latvia
Mauritania
Netherlands
New Zealand
Oman
Philippines
Poland
Port-au-Prince
Singapore
South Korea
Taiwan
Thailand
Ukraine
United Kingdom

International Organizations:

European Union
World Customs Organization

Industry Organizations:

American Association of Exporters and Importers
Business Alliance for Customs Modernization
Joint Industry Group
National Industrial Transportation League
National Customs Brokers & Forwarders Association of America
Retail Industry Leaders Association
U.S. Chamber of Commerce
WCO Private Sector Consultative Group
World Shipping Council

There was also a study that was just recently released this week that I would also provide for the record* to make sure that has an opportunity to be reviewed as well talking about the economic impact that this would have to the global supply chain as well. I think these are important things that we would have had the opportunity to continue to learn had we followed the track of the SAFE Port Act.

Senator LAUTENBERG. There were opportunities for testimony to be given, and I listened with respect. But I will tell you that if this was a brain operation and the doctor said, well, I did not know that I had to have a particular type of tool, I did not know that we used a particular type of anesthesia, fundamental to planning.

*This study, *Global Logistic Chain Security—Economic Impacts of the U.S. 100% Container Scanner Law* is maintained in Committee files.

I had the opportunity run a pretty big corporation before I came here, and we made mistakes. But what happened is we learned that you cannot enter these things, offer a deadline based on the conditions you are describing now. It is absolutely impossible.

When will we have 100 percent scanning?

Mr. AHERN. Well, I would submit to you that is not a wise investment for the taxpayers' dollars. I do not believe 100 percent scanning would equal 100 percent security. I think when you actually take a look at the risk to the global supply chain, the risk for security concerns is relatively low based on intelligence assessments. Given the fact that 90 percent of the global economy moves through the maritime environment, the consequences are high. But I would submit that we have very productive layered defenses in place through the advance information that we are doing a better job of—

Senator LAUTENBERG. Well, OK. We are looking here at a commitment that was made, a very important commitment. We knew that we had to do studies along the way. We knew we had to do tests along the way. It has been 7 years since 9/11. The 9/11 Commission found that the greatest failure in their review was one of imagination.

And when I hear your response to picking a date that has some degree of reliability without a broad explanation of why it cannot be done—can you offer a date with any sense of satisfaction it will be met?

Mr. AHERN. Not with the current technology, not with the economics involved with this, not with the fact that—

Senator LAUTENBERG. OK. What you are saying realistically is that they are going to continue to have to take these risks. There is no other way to assure ourselves that these materials are not included in a container. So you are telling the world here that we cannot do that. This country is not capable of it.

Mr. AHERN. What I am suggesting is that the layered defense approach, beginning with advance information, running it through an automated targeting system, interfacing with intelligence, having the ability to have our Customs-Trade Partnership Against Terrorism be able to do supply chain verification at the point of stuffing, having over 200 officers identified and assigned at the top locations, 58 locations—

Senator LAUTENBERG. I hear you, Mr. Ahern. And I thank you. I think what you are doing is presenting questions now that should have been in the origination of a date and a program.

Mr. AHERN. Well, very respectfully, I would ask that the record be reviewed since the beginning of this process. We have talked about some of the challenges with 100 percent scanning before the law was passed last year.

We thought the SAFE Port Act was a very thoughtful approach and a way to go forward with dealing in a pilot location so that we could learn all the different challenges that are out there.

Senator LAUTENBERG. When does it get done?

I am going to go on to Mr. Caldwell. Four of the world's largest marine terminal operators have indicated on their own that they are going to begin to scan all cargo through their facilities. They are waiting for the administration to set performance standards for

the scanning equipment as Congress required in the 2006 SAFE Port Act. When will these technology performance standards be put in place?

Mr. CALDWELL. Sir, I do not know when those standards will be in place. It is very important to have those standards, and it is important that they be developed through a standard-setting organization such as ISO. Once you actually have those standards, whether it is for NII equipment or RPM equipment, only then can you really independently assess and compare equipment. Then you can compare equipment in another port versus our port? Then you can determine if its capability is less than ours, or if it meets a minimum standard?

I am not sure how the Government or CBP gets that process started within ISO. There is an ISO standard which some port terminal operators have used to certify the general security management in their ports. But there still is not a standard for the actual equipment performance.

Senator LAUTENBERG. So with these terminal operators on their own—what is their target? Does each one make the assessment that they are going to meet the qualities we want in our protection? Or do we keep on waiting for a performance standard that is universal that everyone has to meet?

Mr. CALDWELL. I think these are competitive decisions by these terminal operators. Maybe they see the writing on the wall. They are pushing toward 100 percent scanning, which clearly is in U.S. law at this point, and it would certainly give them a competitive edge if they are able to set up such a system. I do not think any of these terminal operators are claiming they can do this for transshipped items.

Obviously, this equipment is out there. It is being used—advancing the state-of-the-art and hopefully increasing those performance capabilities.

But again, I do not know if there is an active process at ISO to actually set such performance standards.

Senator LAUTENBERG. Mr. Huizenga, do you want to make a comment?

Mr. HUIZENGA. Yes. If you do not mind, Mr. Chairman, I will try to address your concern.

We have been working pretty closely with the industry representatives for some time now. Although we could formalize this—and I think it is useful and we are in the process of doing so, industry representatives are familiar with—the targets that we are trying to hit. The information is out there and we will work with Mr. Ahern's people and the DNDO people at the Department of Homeland Security to formalize this process.

But the more important point is that the technology actually does not exist, despite our best efforts right now. If you want to try to capture an X-ray image or a radiation scan for a transshipped container that comes into Singapore and gets off one ship, gets put on the dock for a very short period of time and then put on another one, there is no space in the terminal to put the equipment. So if you had to take that container and drive it off the port and back through the entry and exit gate, where it is easy to capture the containers, it would completely disrupt the operations of the port.

Despite our best efforts, there are some things that cannot be done and keep the port operating.

Senator LAUTENBERG. But even if the manifest or bill of lading would have been established for each container and some certification that this container is filled with safe cargo, now if the transfer is made without breaking the seal—and I am not intimately familiar with this—does that not take care of it?

Mr. HUIZENGA. It is a simple logistics issue really. The container comes into the port and gets taken off the ship and put down on the dock, and then put on another ship, and it really does not go through a convenient choke point where it can be driven through a scanning device. Now, we are looking for ways to overcome this, but right now we do not have a technology that can solve the problem.

Senator LAUTENBERG. But it would have been driven through a device, to use your expression, before it left the port of embarkation.

Mr. HUIZENGA. It was through a feeder port, perhaps. But that port might not necessarily have been shipping anything directly to the United States. It just adds another layer of complexity to the number of ports you need to try to work at.

Senator LAUTENBERG. Mr. Ahern, any idea what the cost might be to the country to install the necessary equipment to be able to allow our Government to receive the scanning data we need for shipments from overseas?

Mr. AHERN. If we were to look at it globally for 100 percent application, we have over 700 ports around the world that ship to the United States. Obviously, those are pretty large and go down to very, very small feeder ports. We have not actually done a footprint of each one of those 700 ports for the number of terminals and the number of gates that would actually be in each one of these environments. But a rough order of magnitude, we are looking at about \$8 million per lane. A place like Hong Kong, just one terminal has 10 lanes.

That does also not address the issue that Mr. Huizenga spoke about which is transshipment cargo that does not come through the gates. Those are basically on-dock transfers when you have a vessel that comes alongside and takes some containers off to then put on another vessel destined to the United States. There is that complicating factor as well.

Certainly for this initial pilot, the cost of DOE and Customs and Border Protection was about \$30 million each, for a total of \$60 million just to run the pilots in these three very small locations. That was a combination of DOE's resources and capabilities for some of the hardware, the radiation portal monitors, ours for the X-ray, and in one case, Honduras actually capitalized the investment for the X-ray system. So it is a very expensive proposition.

Senator LAUTENBERG. Without being too specific, are the ports that send material to our country rated on some kind of a risk basis? Do we believe that there are ports that are far riskier than others for whatever the reason?

Mr. AHERN. Yes, we do, and there are a couple of additional factors. Certainly the Coast Guard through their HSBIS reviews do ratings. Certainly there is intelligence community assessments as

well, and also we have our own track record now of a number of years of collecting information and doing risk assessment on individual shipments coming from a location where our automated targeting system has rated them above the threshold that requires an examination. We have that data as well. That goes into the compilation of how we would begin to look at a more risk-based approach for particular trade lanes.

Senator LAUTENBERG. I recognize the work that you and your CBP staff have done to set up the scanning pilot program, and there will be some valuable lessons, as you indicated, learned for going forward.

Industry representatives have tried to claim that some security measures like mandatory container scanning are bad for business because they will slow commerce. But I understand that in some ports, including Southampton which you mentioned, after scanning operations were in place, the port actually moved more containers overall. Can you elaborate on that?

Mr. AHERN. Could you repeat that last line again? I am sorry.

Senator LAUTENBERG. Yes. That the port actually moved more containers overall out of Southampton, for instance. Can you tell us whether or not the concerns of the industry are valid, that they will slow commerce to a halt? I think our experience in Southampton said that they see things moving more containers as a result of their inspection.

Mr. AHERN. I would need to look precisely at the numbers or the analysis that led to that conclusion. But I would submit that with a place like Southampton—it is a very small universe of containers coming to the United States. It is an intermittent flow at best. I was just there about 6 weeks ago to look at it again, and it is an 8-acre footprint, which goes to one of the issues. We don't have the environment in most of these ports to be able to put the lay-down of technology so that it could stop at intermittent locations, usually three, to be able to be scanned by the X-ray, the radiation portal monitor, the optical character recognition, and then for the officer in the alarm station to be able to do the review.

There has been some resulting benefit—and this is what I touched on briefly in my oral statement—that if we can reduce that risk overseas, that certainly is one of the exams we do not need to do upon arrival in the United States if there is an alarm that occurs. We then have the ability through the information we have collected to transmit that whole electronic file with the radiation spectra, the X-ray image, as well as the automated targeting systems in one electronic file to our domestic location, Newark, for example, to be able to say we did have an alarm. We did resolve it before it came. That is a very, very small manageable universe.

Senator LAUTENBERG. Right.

Mr. AHERN. That is one of the challenges to try to put the—

Senator LAUTENBERG. Did that slow the pace? The work done there—does that slow the pace of movement?

Mr. AHERN. I would submit there was no pace to disrupt in a place like Southampton. It was such a small, intermittent type traffic that shows up at the gate. It is such a small universe.

In a place like Hong Kong, for example, 1.2 million containers roughly a year to the United States. Through each one of those

gates, you are running 300 containers an hour through those gates. To be able to review the image, to be able to read the spectra, to be able to go ahead and do any resolution would add exponentially to the traffic and throughput through those gates. That is where we see the problems. It is not so much—

Senator LAUTENBERG. So 300 containers an hour move through there.

Mr. AHERN. In a place like Hong Kong, that is where—

Senator LAUTENBERG. Yes, but electronic readings, however they get them, for each container—inspection is done electronically, technologically. Right?

Mr. AHERN. In Southampton, yes. And in Hong Kong, just one lane of one terminal. And the normal throughput through all the lanes is about 300 per hour.

Senator LAUTENBERG. Oh, all the lanes. OK, I am sorry.

Mr. AHERN. Per lane over all of the lanes. So it would be 300 times the 10 per hour coming through those facilities.

Senator LAUTENBERG. OK.

Mr. AHERN. But what the problem is—and we saw this even when we went back to the Hong Kong demonstration project called ISIS about 3 or 4 years ago, when there were claims and representation that it was providing 100 percent scanning, I also had an opportunity to see that personally as well. They were scanning. They were just running containers through X-ray and radiation portal monitors with no regard for the quality of the image or any resolution of the image that was occurring through this demonstration project through industry.

Each one of these technological systems has to be manned at this point in time for somebody to look for the anomaly. Otherwise, the complementary package of an X-ray with a radiation spectra to see if there is any shielding of a harmful isotope is going to be negated. So it has to have the human intervention, a trained officer to look at the image to see if there is an anomaly that could be there hiding an isotope of concern.

Right now what does not exist—and this is one of the challenges we see very significantly that is in the report—is an anomaly recognition software so you do not have to spend 3 to 5 minutes per image to see if there are anomalies that are out there.

Senator LAUTENBERG. It sounds fairly basic in terms of—if it needs human intervention, obviously it is going to be different. I am assuming that some kind of an alarm system that picks out the particular thing that has got to be called attention to would be operated also through the system that does the analysis.

Mr. AHERN. There is a system for an alarm if an isotope is identified. Those alarms are actually identified through the radiation spectra capabilities. What is not existent is the complementary package for the nonintrusive inspection capability, the large-scale X-ray. There is no alarm capability there that identifies that there is an anomaly in this particular box without getting into too much detail. That is what is going to be a critical piece to make this integration of these technological packages a success, that each one have a software capability to be able to alarm someone, whether it be our presence overseas, which we would advocate—

Senator LAUTENBERG. That being the case, do the concerns of industry register a problem that is real, that it would bring a halt to commerce?

Mr. AHERN. In my estimation and in my experience and my observation of the three pilot locations and also looking at Hong Kong, if we were to apply this in a universe of 100 percent environment and each one of the alarms needed to be resolved and each one of the X-rays needed to be determined by a trained officer, it would bring commerce to a halt.

Senator LAUTENBERG. Well, Mr. Huizenga?

Mr. HUIZENGA. And I just want to add, if I could, one clarification. In Southampton, I think it is fair to say, that the gate traffic, the containers coming into and exiting the terminal—it really did not impact the operation.

But the transshipped containers in Southampton were really not inspected according to the requirements of the SFI. It was not possible in the end. We ended up having to do some workarounds. So it is another example of, although the gate traffic is pretty easy to get, the transshipped containers were still difficult to—

Senator LAUTENBERG. Yes. Well, but I am not sure about the message we are sending out of here. We obviously need the commerce. We need the activity of shipped materials. Enormous traffic.

Is it suggested that we cannot be as safe as we should be and still have the movement of material?

Mr. AHERN. Mr. Chairman, I would submit a few factors for consideration.

First, the security systems—the layers we have in place post-9/11—have actually been very effective and they continue to improve. We thank GAO for their continued reviews. Each time they come, we find additional enhancements. For our 24-hour rule, where we get advance information, we have a final rulemaking about to come out that will get additional information in advance of shipments so that we can run that through our targeting systems to identify shipments of concern.

I think it is also important, as we look at our partnership with industry, the security protocols they have put in place, beginning at the onset of the supply chain, at the point of stuffing which is the greatest opportunity for the introduction of a significant piece of material that could be of concern or a weapon or other contraband of concern—that is continuing to get better.

I think it is also important to realize that when we began this, we did have any radiation portal monitors here in the United States. We had one that was being demonstrated over 4 years ago in Detroit. We now have 98 percent. 98 percent of the container traffic coming to the United States, before it goes into the commerce of the United States, actually goes through radiation portal monitors before it departs the terminals at the ports within the United States. That is a significant accomplishment.

As we continue to go ahead and balance the security responsibility, we also need to balance it against the risk. The continual threat assessments show that the risk in the maritime environment is relatively low. Certainly the consequence is high. And I would submit with the risk reduction strategy we have in place, I believe it matches what the risk would be.

Now you weigh that against the consequence, the economic consequence, of the layering of 100 percent scanning globally, I think that is a huge consideration, and we need to make sure, as we are putting security protocols in place, that we are not going to give the terrorist organizations an opportunity to claim victory because we responded in such a way that is going to drive up costs so significantly.

And finally, I think we need to be mindful of the fact of the consequences that really are out there looming large. I again ask this committee to take a look at the report released by the World Customs Organization and look at the submissions by the trade industries, the international organizations, and our international partners. They are calling for reciprocity. So your port in New Jersey, sir, would be one that they would say if you want us to do 100 percent scanning destined to your country, we want the same reciprocal requirement from you. You talk about logistics and movement to the trade community here in the United States that exports, the impact that will have on the trucking industry, the rail industry, the maritime industry, the footprint to be required here in the United States. It is a huge issue that has not even been studied from an economic standpoint as we look at 100 percent scanning overseas. Our foreign partners are saying we are just as concerned with things coming from the United States. And that really should be considered as well, sir.

Senator LAUTENBERG. Well, but there were things said a few years ago about our ability to get the 100 percent scanning, implying there that that would be 100 percent safe, 100 percent secure.

Now, when you talk about the money being spent, look at what we spend on baggage screening for airplanes. There is an entire industry now that is related to having to provide that kind of security and safety.

But as I hear you now, Mr. Ahern, I am concerned that the message is, well, we cannot do it. If that is the case, then I am going to ask for a comprehensive report from your Department that tells us what can—I want the public to hear from the people who have the authority, have the responsibility, have the resources to do it to tell us exactly what the score is here.

I want to just ask a question here. I understand that CBP is receiving container scans now but that an individual person has to look at each one of them to see if they present a security risk, the thing we have just been talking about. So what does the Department do now to develop the technology for, as I suggested earlier, automatic detection? Can that be achieved?

Mr. AHERN. Right now that has been a real technological challenge for industry, and we certainly have been—the medical industry has been challenged by this issue for a number of years before we had this issue emerge as a homeland security problem. We do not have the solution to that within Homeland Security. We really challenge industry to come up with that software anomaly recognition package. That is going to be the key to make this go forward.

I also would submit, back to your previous question of mixed messaging, I hope that is certainly not the case. But just to clarify again here, I believe, to make sure the country realizes, the security measures that are in place I believe provides a layer of secu-

rity that is appropriate and continue to enhance each one of the layers.

And as we look forward, I would believe that we need to take a look—to continue the risk layers in appropriate ways in a place like we currently have in Pakistan where we have a protocol in place where we actually screen 100 percent of containers coming out of just one of the ports in a place like Qasim, Pakistan. We certainly think it would make sense to take a look at another location right there out of the same country, a place like Karachi. We need to make sure that we start to have a thoughtful approach to 100 percent scanning where it makes sense in high-risk trade lanes so that we can actually provide an additional layer, where we do not think the current five layers of risk reduction are sufficient.

Senator LAUTENBERG. Yes. Well, it raises a question that is not going to be resolved this day in this hearing.

Are we saying that there is a limit to the amount of protection that the public can be afforded? And I am not talking about afforded in price. I am talking about afforded in functioning. We have so much of our resources now helping us to defend against terrorist attack, against malicious targeting with very high-powered weapons. Do you want to comment? Do you want to give us an index of how safe we can be?

Mr. AHERN. I will give several points for consideration.

First off, no one should be misled to believe that 100 percent scanning with the current technology that is out there or anything we see on the horizon is going to provide 100 percent security. No one should be misled by that point.

The other thing is certainly we need to realize there is risk that needs to be assumed in every environment. The maritime environment is not excluded or separate alone. I mean, certainly it is a global impact economically, but certainly even with the layers, even with 100 percent scanning thrown on top, you still will not reduce the risk 100 percent. That has to be an assumption going forward.

My biggest concern, with 32 years of experience, is we are focusing in the maritime environment to the exclusion of other areas of higher concern to this country and continue to invest time, efforts, and resources in the maritime environment where have other concerns that we need to have the funding, the resources, and our technological attention directed toward. I will be meeting with you this afternoon, sir, to talk about rail security. That is another environment we have other concerns about. So we need to take a look at the borders and border security in its totality, not just continue to focus on one particular aspect of homeland security in one particular vector.

Senator LAUTENBERG. Do you want to add something, Mr. Caldwell?

Mr. CALDWELL. Yes, Senator Lautenberg. In my portfolio, I do have other areas of maritime security beyond the CBP programs, to include Coast Guard programs. Based on this other work, I share some of Mr. Ahern's concerns. I would not want to see 100 percent scanning become the "Masinot Line" of maritime security. You are putting all your resources in a certain type of attack in a certain vector. Those resources could also be used to protect maritime areas that are relatively unprotected now, such as bulk car-

gos, small vessels, or attacks in the maritime environment by other means.

Senator LAUTENBERG. I remind you, before we close this hearing, that we spend over a quarter of a trillion dollars, close to a half, on a war that is supposed to protect us against terrorism. That is what we say. Now, if we were to place the same emphasis financially on protecting us from an invasion through the shipping structure, might we solve the problem? Mr. Ahern, you mentioned money several times. And I agree. We have got to put it where our interests lie. But I do not see it happening right now, but I do see us spending the money in Iraq and Afghanistan and other places around the world. But we have not had the kind of loss that we had on our own shores at 9/11, the number of people that lost their lives in my neighborhood, if you will.

So there is something here that I think would be of significant public interest, and that is, we are saying—or the Administration is saying—you are representing their view and their determination—that we cannot expect the kind of result that we were led to believe we would get. That was the assumption. The 100 percent inspection was thought to be, if not 100 percent safety, that we were very close to that kind of a protection wall.

So whatever you have got to develop for us, Mr. Ahern, I ask you to do so and be blunt so that the public understands what is happening now in this Administration and in our world.

Thank you. This Committee hearing is adjourned.

[Whereupon, at 11:06 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF AMERICAN ASSOCIATION OF EXPORTERS AND IMPORTERS

Chairman Lautenberg, Ranking Member Smith, and Members of the Subcommittee,

The American Association of Exporters and Importers (AAEI) appreciates the opportunity to offer its comments on U.S. Customs and Border Protection's (CBP) Secure Freight Initiative (SFI) and its other supply chain security efforts.

AAEI has been a national voice for the international trade community in the United States since 1921. Our unique role in representing the trade community comes from our broad base of members, including manufacturers, importers, exporters, wholesalers, retailers and service providers, including brokers, freight forwarders, trade advisors, insurers, security providers, transportation interests and ports. Many of these enterprises are small businesses seeking to export to foreign markets.

AAEI is truly a member driven organization. In AAEI's committees, conferences and working groups, the professionals who make up our membership spend hours sharing their trade facilitation, supply chain security and other international trade experiences with other professionals and learning from the experiences of others. Through those activities, our members are able to coalesce around those experiences into an in-depth analysis of important international trade policy issues and provide that insight to policymakers in Washington and throughout the world.

AAEI is deeply interested and vested in the subject of this hearing. We have multiple concerns regarding the effectiveness, efficiency, significant costs, practicality, and real world benefits of SFI initiatives and other government mandated efforts such as 100 percent scanning. We hope that the practical experience of our members in compliance, trade facilitation and security will be of assistance.

While AAEI remains very concerned about the implementation of 100 percent scanning on a global basis,¹ we believe the prototype testing undertaken in implementing SFI to be a correct approach to the development and implementation of important supply chain security programs. The development and implementation of such important and complex programs requires comprehensive testing to, ensure that the programs will effectively and efficiently provide the enhanced operation that we all desire and recognize, as intrinsic to achieving immediate and long term economic and homeland security benefits. Implementing 100 percent scanning or any other universal data submission project without such a prototype may unnecessarily result in gridlock at the ports, the submission of overwhelming volumes of data and the expenditure of enormous public and private resources reengineering solutions to problems that could have been, and frankly must be, avoided. As export/import enterprises, it has been our experience that testing proposed security programs using real world systems and processes is not only necessary for successful implementation but critical to the determination of what, if any, increased security can be obtained.

In our comments on CBP's January 2, 2008, Notice of Proposed Rulemaking, we urged CBP to fulfill its obligation under the SAFE Port Act to test the "feasibility" of its proposal by undertaking just such a prototype before implementing the 10+2 advanced data requirements. Unfortunately, CBP has steadfastly refused to conduct a full pilot of its 10+2 proposal, instead running a very limited prototype.

AAEI believes that a pragmatic "holistic" approach to trade security is paramount. This committee's grasp of commercial and technological realities is of great value in understanding and dealing with multiple independently created public and private sector initiatives each intended to address vital homeland security related issues. Your jurisdiction both requires and enables exploration at the increasingly difficult intersection of compliance, facilitation, safety, and security.

¹ Among our concerns are that each and every one of the statutory performance and implementation criteria are met. See 9/11 Commission Act Section 1701(b)(4).

As the Committee knows, there are numerous trade security efforts that directly impact vital U.S. supply chains. These programs include supply chain partnerships, data collection, advanced data methods, related security program elements and 100 percent scanning, among many others. The depth and extent of these programs can be seen in AAET's now familiar *American Trader's Guide to Post 9/11 and Homeland Security Programs*. (A copy is attached.) Also available at <http://www.aaei.org/aaei/files/ccLibraryFiles/Filename/000000003019/TSP%20FINAL%20%2801-16-08%29.pdf>.

Initially released in the Fall of 2007, and recently updated to include the "10+2" information, the Guide is the product of extensive discussions and review with policymakers, industry observers and trade professionals. The Guide provides trade professionals with one piece of paper showing the vast number of the trade security programs that companies have to deal with. You will notice that the single sheet of paper is not a standard size sheet. In order to make the list of trade security programs fit on a single sheet of paper, we had to use a larger size. In fact, we had to go to two pages!

The Guide provokes one of the fundamental security questions of the Post-9/11 age: How many layers of security are enough for risk management to work?

AAEI supports the risk management concept of "defense in depth." We believe that the best security is derived from an approach in which well integrated security programs are layered together to create a web of defense against terrorism. To be well integrated, the layers of such a defense must not unnecessarily overlap, or leave gaps. Layers should not be added if they provide no demonstrable security gains. In fact, such layers are likely to undermine security as they take scarce resources of time and money from the layers that do provide security gains.

While each program listed in the Guide may have provided valuable security initiatives when they were implemented or even when viewed in isolation, the Guide makes clear that, these programs have, with the best of intentions, been introduced without being integrated into existing regulatory legislative or private sector designed structures. In fact, they have emerged from multiple Congressional committees, Government Agencies and private sector initiatives with limited policy consultation amongst these diverse "entities". Thus, both DHS/CBP and the trade community face an expanding trade security environment of unnecessarily burdensome, complex and often overlapping programs. With the complexity and overlapping nature of the current security environment, programs that, on their face, may appear to increase security may actually provide no measurable security gains.

This point can be best illustrated by examining the security environment of a single supply chain.

Let's look at security layers that are applied by U.S. CBP to a container exported from Pakistan's Port Qasim to a validated C-TPAT participant in the U.S. today.

Layer 1: As a validated C-TPAT participant, information about the participants in the supply chain and their security practices have been provided to, and validated by, U.S. CBP. CBP has validated that the C-TPAT participant is utilizing the supply chain security "best practices" that have been identified by CBP. CBP's validation of this information is done prior to the container's arrival at the port of export.

Layer 2: Once a specific shipment has been initiated, the container is prepared and sent to Port Qasim. According to CBP's Secure Freight Fact Sheet, when the container arrives in the port, officials of the Pakistan government subject it to passive radiation detection equipment and non-intrusive inspection (NII) equipment. The NII uses "x-rays or gamma rays to penetrate the container and produce an image of the contents." The output of these scans is integrated with other data available to the terminal operator, the Pakistani government (including export declaration data which is also sent to CBP), and in other governmental systems. The image of the content and the other integrated data is electronically provided to CBP's targeting system in real time. CBP personnel are able to examine that information to determine whether the contents of the container present any threat.

Layer 3: Twenty 4 hours prior to the loading of the vessel, the vessel carrier must provide CBP with manifest information through CBP's Automated Manifest System. That manifest information includes the names of the parties involved in the transaction, a description of the goods and other shipment and transportation data.

Layer 4: Within 24 hours of arrival at the U.S. port, the validated C-TPAT importer will pre-file its entry summary in order to get the benefit of CTPAT's lower targeting scores. Again, the entry summary contains much of the same

basic information that has been provided in the three previous layers described above (*e.g.*, names of the parties, description of the goods etc.)

Yes, there are data differences between the various layers, but the vast majority of the information is the same. Moreover, for repetitive shipments of the same commodity between the same parties, the redundant data will be provided over and over again. This is in direct contradiction to one of the principle goals of ATDI—an account based approach to homeland security, which would greatly reduce the need for redundant data to be submitted to the government over and over again.

On January 2, 2008, CBP proposed a 5th data layer—the “Importer Security Filing and Additional Carrier Requirements” proposal (also known as the 10+2 proposal). This layer would require the U.S. importer (regardless of CTPAT status) to file a Security Filing (SF) to CBP 24 hours prior to the loading of the container on the vessel. The filing of the SF is required without any consideration being given to whether: (1) the importer is validated C-TPAT member; (2) that much of the same basic information from the same sources has already been provided by or on behalf of the importer; or (3) whether the shipment is being exported from a SFI port that provides CBP with a real time image of the contents of the container before it is loaded on the vessel.

As just one example, AAIE believes it is unnecessarily duplicative to require the submission of the “10+2” line by line targeting data 24 hours prior to vessel loading from low risk importers on shipments that have already been subject to: (1) C-TPAT validation; (2) radiological scanning; (3) content image scanning; and (4) the filing of manifest data. Thus, for C-TPAT shipments from SFI ports, no 10+2 submission should be required.

AAIE urges the members of this subcommittee and other Members of Congress to require CBP to take a holistic approach to supply chain security and integrate the plethora of security programs into a cohesive program that provides quantifiable risk reduction in light of the true risks posed by terrorists.

We thank you again for allowing us to submit these comments. We look forward to providing you with further information at your request, and stand ready to assist in any way possible.

*This chart is a work in progress. Categories B and C reflect general consensus and are SME oriented. Thus, they underrepresent larger and multinational companies.



PREPARED STATEMENT OF RENEE STEIN, CHAIR, AND RICHARD M. BELANGER,
COUNSEL; BUSINESS ALLIANCE FOR CUSTOMS MODERNIZATION*

The Business Alliance for Customs Modernization (BACM) submits this statement to the Senate Commerce Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety and Security regarding its hearing June 12, "Supply Chain Security: Secure Freight Initiative and the Implementation of 100 Percent Scanning."

BACM is a coalition of U.S. companies that import and export extensively, filing over two million entries valued at more than \$130 billion per year. It is dedicated to modernization of U.S. customs laws, regulations and policies and committed to the facilitation of trade to the greatest extent possible consistent with customs compliance and trade security.

BACM members strongly support U.S. Government efforts to make the global supply chain more secure in the post-9/11 environment. We have eagerly participated in forums like the TSN and COAC and have participated in the development of programs such as C-TPAT and the 24-hour rule. What makes these programs so successful is that they were developed cooperatively with the trade to target security risks without creating unnecessary burdens for businesses. While BACM members have faced increased costs as part of these efforts, we support these programs because they achieve the critical balance between our national security and economic interests.

BACM members object, however, to additional security requirements for shipping when the security benefit is negligible and adds an unnecessary burden to industry. We are concerned that, in its desire to protect our borders, the U.S. is enacting layer upon layer of security programs without consideration of how they reconcile with each other or whether they create burdensome redundancies. The 100 percent scanning requirement raises this question. If CBP will be requiring the trade to perform extensive data reporting under the 10+2 initiative to identify high risk cargo for further scanning, how does this reconcile with the 100 percent scanning requirement once implemented?

We urge the Committee to give serious consideration to these issues in order to avoid putting U.S. companies at a competitive disadvantage through compliance costs that are economically and logistically burdensome and yield no appreciable additional security benefit.

The Security and Accountability For Every (SAFE) Port Act of 2006 (P.L. 109-347) created the Secure Freight Initiative, a pilot program for 100-percent screening of inbound containers at three overseas ports. The program combines non-intrusive inspection imaging with radiation portal monitors to identify any anomalies in shipments destined to the United States and to target those containers for further inspection. The program has now been tested for a limited time in smaller ports in Honduras, Pakistan and the United Kingdom and has been found by CBP to have significant technical, operational, resource-related shortcomings. Of high concern is the fact that the computer technology and capacity does not exist for quickly and accurately identifying anomalies in shipments, particularly for transshipped cargo.

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), requires 100 percent screening of all imported containers by non-intrusive imaging equipment and radiation detection equipment by July 1, 2012. With this hearing, Congress is looking at how to reconcile the SFI pilot results with the mandates under the 9/11 Commission Act. We hope that the Congress will delay implementation of the 100 percent scanning requirement until the technology is available to ensure quick and efficient scanning that does not cause burdensome congestion in port operations overseas.

The SAFE Port Act of 2006 also instructed CBP to evaluate whether additional cargo information would be needed to better evaluate shipment risk. In response to this mandate, CBP has recently proposed its so-called "10+2" data elements proposal, which would impose extensive new data reporting requirements on shipments to the U.S. 24 hours before lading at foreign ports. The purpose of 10+2 is to prevent smuggling of weapons of mass destruction into the U.S. and enhance cargo safety before goods are loaded onto U.S. bound boats. If CBP identifies an anomaly in the data reported, the cargo is then subject to scanning to better identify whether there is a threat to U.S. commerce.

*American Honda Motor, Archer Daniels Midland, BP America, Caterpillar, Chrysler, Ford Motor, General Electric, General Mills, General Motors, Hanesbrands, Hewlett Packard, Home Depot, IBM, J.C. Penney, Limited Brands, Lowe's, Mattel, Microsoft, Nike, Nissan North America, Sears, Shell, Sony Electronics, Target Corporation, Toyota, Wal-Mart

The mandate for the 10+2 proposal was enacted before Congress passed the 100 percent scanning requirement. It is now clear, however, that the two programs together overreach. The 10+2 was meant to help CBP target suspect cargo for scanning. The 100 percent scanning requirement would render the 10+2 additional data elements redundant or useless.

BACM has submitted public comment on CBP's 10+2 program, expressing significant concerns that the program would impose commercial costs and delays, putting U.S. companies at a competitive disadvantage in the global economy. Our concerns are many but can be summarized as follows:

1. there has been no demonstration to the trade community as to how this proposal would measurably improve supply chain security;
2. the proposal moves away from risk management principles as the necessary solution to burgeoning trade flows, legitimate regulatory needs and limited or static resources;
3. the proposal treats all shipments for all sources as the same, without regard to trusted partner or authorized economic operator programs such as Customs-Trade Partnership Against Terrorism (C-TPAT) and more secure trade;
4. for many shipments 10+2 requires reporting combinations of the same data attributes over and over again, resulting in redundancies and the overload of repetitive data;
5. in many cases, the newly required data elements are not known or readily available as early in the supply chain as the proposal assumes;
6. 10+2 reporting requirements would ignore account-based processing that is the basis for the Automated Customs Environment;
7. the proposal seriously underestimates the costs that would be imposed on business; and
8. it would not address a number of logistical and processing issues that need clarification before moving forward
9. a true-to-life prototype should be conducted using representative importers of different sizes and from different industries in order to learn more about how the proposal will work when CBP collects the data according to proposed rules and conducts actual targeting.

We believe that these concerns should be addressed before the Administration moves ahead with the 10+2 initiative. More broadly, it is critical that coherence be brought to the entire spectrum of supply chain security programs.

We agree that it is imperative that the U.S. Government work to eliminate container vulnerabilities, but it must not be done by piling on layer after layer of initiatives with little added security benefit. Congress must work to reconcile all of the security initiatives currently in place to ensure a more fluid and complementary system that is not overly burdensome to the trade. Serious consideration must be given to the cost and benefits of each new security system before the Congress and Administration impose additional burdens on the industry. Such concepts as reporting exemptions for low-risk shipment and account-based filing for repetitive shipments are examples of provisions that might better reconcile the overlapping security mandates.

We appreciate the opportunity to submit this statement. Thank you for your consideration of our views.

PREPARED STATEMENT OF CATHERINE ROBINSON, ASSOCIATE DIRECTOR, HIGH TECHNOLOGY TRADE POLICY ON BEHALF OF THE NATIONAL ASSOCIATION OF MANUFACTURERS (NAM)

The National Association of Manufacturers (NAM) is providing the following written statement for the record of the Committee on Commerce, Science, and Transportation; Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security Hearing "Supply Chain Security: Secure Freight Initiative and the Implementation of 100 Percent Scanning" held on June 12, 2008. The NAM represents a broad spectrum of U.S. manufacturers, with members in every industrial sector and every state. Its membership includes both large multinational corporations with operations in many foreign countries and small and medium manufacturers that are engaged in international trade on a more limited scale. Our members depend heavily on imported parts, components and finished products to compete not only in the U.S. marketplace but in foreign markets as well.

NAM members recognize the important role Customs and Border Protection (CBP) plays not only in protecting the United States but also in facilitating legitimate trade. Our members are committed to working with CBP and other U.S. law enforcement agencies to keep America secure and safe from terrorist threats and other security challenges. Many NAM members gladly participate in the numerous CBP initiatives that make the United States more secure.

This hearing is timely as CBP is currently working on a number of new initiatives. While the NAM supports the efforts of CBP, we want to ensure that new customs requirements achieve the dual CBP goals to “enhance national security while protecting the economic vitality of the United States.” The NAM recognizes the difficulty of striking the right balance between the two. We believe, however, that protecting national security and facilitating international trade need not be mutually exclusive.

Striking the right balance between enhancing national security and facilitating trade is critical. Manufactured goods accounted for 76 percent of all imports into the United States in 2007, or \$1.9 trillion. U.S. manufacturers have global supply chains, source inputs from around the world, and import parts and components on a daily basis. Many have developed “just-in-time” supply chains to stay competitive in today’s global economy. Therefore, any new programs developed by CBP must be mindful of the way U.S. manufacturers operate their supply chains and their important role in the U.S. economy. New programs should be real world tested to guarantee that they are both fully effective from a security perspective and do not place U.S. manufacturers at a competitive disadvantage vis-a-vis their competitors around the globe.

In order to strike the right balance, CBP must implement new programs based on sound risk management principals. Low-risk cargo from trusted, fully-vetted shippers should be treated differently than high risk cargo. CBP should not implement programs that treat the two identically. Doing so wastes limited resources on containers and companies that have been validated by CBP, and leaves insufficient resources to focus on the higher risk shipments.

The NAM welcomes this Committee’s and others’ interest on customs programs. There are a myriad of customs issues that merit attention including resources for CBP, technical issues such as duty drawback, interagency cooperation, international recognition, intellectual property rights and supply chain management programs such as C-TPAT. While those issues are deserving of increased attention, the NAM would like to focus our statement on the issue at hand—100 percent scanning and how it relates to current CBP initiatives such as the so-called Customs 10+2 proposed rule.

While 100 percent scanning remains a controversial and problematic issue, the NAM believes in the Congress’ approach to testing 100 percent scanning through a serious pilot program around the world before requiring U.S. manufacturers to change business models globally. Real-world testing is critical for new programs of this magnitude. The 100 percent scanning pilot program has already proven useful as it has shown the government where the problems lie, what needs to be improved or changed, and, most importantly, that the government lacks the capacity to process the breath of information provided by 100 percent scanning. Specifically, CBP stated in May 2008 that the 100 percent scanning pilot program has already shown that the initiative is cost prohibitive for three reasons: (1) the cost of the necessary technology is extreme; (2) the bandwidth requirements for the scanned images are too great; and (3) the cost of the personnel to review the images and run the program is exorbitant.

We believe the 100 percent scanning pilot program provides an excellent precedent for current CBP initiatives and strongly believe a real pilot program is needed for the proposed 10+2 rule. The proposed 10+2 rule will also drastically change the way U.S. manufacturers operate, even more so than the 100 percent scanning mandate—entire supply chains and just-in-time delivery systems will be undone by the proposed rule. Yet, CBP has indicated it will not conduct a pilot program before a final rule is implemented. We are aware of no test, including the Advance Trade Data Initiative (ATDI), that is being run that tests from end to end the many requirements of the proposed rule. Failure to conduct a pilot program will have severe negative consequences to the U.S. economy and our national security.

The NAM is not opposed to the intent of the proposed 10+2 rule. However, as currently drafted the rule not only fails to enhance national security, it also fails to facilitate trade by greatly increasing the cost of doing business for U.S. manufacturers—achieving neither of CBP’s dual goals. The NAM has offered to CBP several specific ideas to improve the rule including testing it through a pilot program and providing benefits to C-TPAT members. Our recommendations have thus far not been heeded.

As this hearing has shown, pilot programs are critically important. NAM members stand ready to comply with 10+2 and to invest hundreds of billions of dollars to change their operations. However, before NAM members invest the money, they would like to know that the program will not be changed 6 months after implementation to correct some of the deficiencies in the program. A pilot program would prevent manufacturers and the government from having to make multiple changes to their operations. Additionally, it would allow the government to address the security risks that will arise from implementation of the proposed rule (*i.e.*, containers sitting in foreign ports for several days waiting to be loaded on vessels).

In the Safe Port Act of 2006, Congress instructed CBP to develop a way to collect more data in advance of lading for which CBP proposed the 10+2 rule. Then in 2007, Congress mandated that every container coming into the U.S. should be scanned to provide CBP advanced data before lading by 2012. Implementing both programs is not only unnecessary but also an inefficient use of limited government resources. The NAM believes now is the time to evaluate rigorously all customs programs and to take a holistic approach to national security. Redundant programs should not be implemented.

The NAM supports the 100 percent scanning pilot program and believes it sets the correct precedent for real-world testing on other major CBP initiatives. The NAM asks that the proposed 10+2 rule also be real-world tested before final implementation. Phased-in enforcement is no substitute for a pilot program.

NAM members are committed to working with CBP to keep America secure from terrorist threats. However, new programs and initiatives must be based on risk management principles in order to enhance national security and facilitate trade. National security and economic vitality are not mutually exclusive and the NAM firmly believes the right balance can be struck to achieve the dual goals.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK. R. LAUTENBERG TO
JAYSON AHERN

Question 1. In your April report to the Appropriations Committee on the SFI pilot, you stated that over 13,000 data filed from the three operational ports had been successfully integrated, transmitted and received. This is no small feat in technologically and you should be lauded for your progress in this area. What is that total number to date?

Answer. Since October 2007, SFI has scanned 237,054 containers in Southampton, U.K., Port Qasim, Pakistan, and Porto Cortez, Honduras.

The scanned images and associated data captured by SFI's integrated scanning system at the foreign ports have been transmitted back to the National Data Center and fused with trade data required by the 24 hour rule and made available to all Customs and Border Protection (CBP) Officers with access to Automated Targeting Systems ATS. CBP Officers stationed at SFI or CSI ports, the NTC-C, or at domestic ports (ATU's) are able to access the additional data when determining the potential risk of U.S. bound shipments from SFI locations.

Question 2. In all of the pilot locations, you experienced significant concerns with labor over the safety of scanning equipment and concerns about potential radiation exposure. While you mention the DHS has conducted extensive studies on the occupational safety of this equipment, is your research and findings supported by the National Academy of Sciences or the National Institutes of Health? You mention in your report that several studies have been conducted on this issue, can you please provide for the Committee what specific studies you are referring to?

Answer. There have been several independent studies of health and safety issues related to the SAIC P-7500. CBP and the U.S. Department of Defense have concluded that the drive-through P-7500 does not pose a threat of radiation exposure to drivers, operators or by-standers. SAIC has also conducted tests to ensure that its equipment is within the radiation dose limits set by the International Council of Radiation Protection. Results of these tests have been published and presented to foreign governments.

One of the hurdles in operating scanning equipment overseas has been the regulations pertaining to radiation exposure in foreign countries. Upon placing imaging equipment in Southampton, U.K., CBP was informed that the P-7500 must comply with the United Kingdom Health and Safety Ionizing Radiation Regulations (IRR) of 1999. To comply with the regulations, a Radiation Protection Advisor was contracted to train and certify four CBP officers to become on-site radiation security officers. Additionally, an independent study conducted by NUKEM (the designated U.K. radiation compliance company for Her Majesty's Revenue and Customs and the Southampton Container Terminal), evaluated and tested the P-7500. Their conclu-

sions mirrored the same positive conclusions as other independent studies stated below. Her Majesty's Revenue and Customs also posted a letter on a trade webpage describing the safety features of the P-7500, along with the radiation safety testing performed by NUKEM. This letter certified that the P-7500 does not pose any radiation hazard to truck drivers, operators, or bystanders when operated and maintained properly.

Another hurdle in using scanning equipment overseas has been the safety concerns of the personnel operating the equipment. In Southampton, U.K., and Busan, Korea, truck drivers and their unions were concerned about possible exposure to radiation while driving through the non-intrusive inspection (NII) equipment. Therefore, CBP published fact sheets describing the safe operation of the P-7500 and the numerous tests conducted and the outcomes. These fact sheets were distributed to the terminal operators' employees, truck drivers and their unions. To further prove that there is no radiation risk associated with the P-7500, CBP health physicists were commissioned to supply dosimeters to the CBP officers in Southampton. These dosimeters are rotated through Southampton and are evaluated in Indianapolis on a quarterly basis.

To date, the National Academy of Sciences and the National Institute of Health have not conducted any studies that would challenge the findings of our tests.

Question 3. In your testimony you stated that in both 2005 and in 2008 GAO reported that CBP's human capital plan did not appropriately determine the optimal number of CBP officers needed at each CSI seaport to effectively carry out its duties. Do you know if the human capital plan has yet been modified since you released your report on the CSI program in January?

Answer. CBP completed a study that determined the optimum number of Targeters for each CSI port based on the volume of shipments and risk considerations. The total number of CBP personnel who can be stationed at the overseas CSI locations is limited by a host of factors. *i.e.*, the U.S. Department of State (DOS) determines the number of U.S. personnel that can be stationed abroad. DOS takes into consideration the number of U.S. personnel that are already stationed abroad and how the increase in the numbers would benefit the U.S. They also consider whether the host nation will request an equal number of their own government personnel to be stationed in the U.S. receiving the same Privileges and Immunities granted to U.S. personnel. The staffing allocation model has been adjusted by stationing Targeters at the National Targeting Center to support CSI operations by pre-screening and targeting shipments that cannot be handled due to the reduced number of Targeters actually stationed abroad. The Targeters at the NTC-C would be screening Bills of Lading that are below a certain threshold, in order allow the CSI Targeters to concentrate on shipments that have a higher score on the ATS. This allows the CSI Targeter more time in developing additional information to substantiate or negate the risk of the targeted shipment. The GAO was presented with this Staffing Allocation Model on October 2007. This information is For Official Use Only (FOUO).

Question 4. What is the national policy of Canada and Mexico with respect to scanning of inbound cargo containers? Does Canada and Mexico have a scanning requirement to prevent weapons of mass destruction from entering their ports of entry in cargo containers? If either nation does have such a requirement, is it stronger or weaker than the U.S. requirements for the scanning of inbound container cargo?

Answer. *Canada:* Canada uses risk-management systems and processes to screen, scan and release goods rapidly while ensuring safety and security. Targeting is an approach for identifying potentially high-risk goods for examination. The Canada Border Services Agency's (CBSA) targeting activities are multi-faceted, multi-dimensional and embedded in virtually every area of the organization. Goods can be targeted before they come to Canada, upon arrival, and in some cases, post-arrival. For example, under the Advanced Commercial Information (ACI) system, marine and air carriers must transmit conveyance and cargo reports for all vessels and aircraft loaded with commercial goods destined for Canada. Targeters use this data to search for health, safety and security threats before the vessel or aircraft arrive in Canada. Targeters also review the risk scores and cross-reference suspicious cargo against a number of data bases to determine whether an examination should follow. If a container is selected for examination, Canada may elect to use a mobile Vehicle and Cargo Inspection System (VACIS) to detect irregularities in the shipment. The mobile VACIS is a truck-mounted, gamma-ray scanning system that captures an image of a marine container, rail car or truck contents. Other detection equipment that the CBSA employs may be in the form of imaging equipment, explosive detectors and radiation detection technologies.

Mexico: Through bi-national agreements allowing for the sharing of best practices with CBP, Mexico has developed a national policy very similar to that of the United States in that it utilizes data analyses to target high risk shipments. Under this strategy, Mexico Customs presently runs 69 cargo non-intrusive inspection (NII) equipment sites nationwide. At present time, 100 percent of rail shipments and 90 percent of all empty inbound conveyances are scanned at Mexico's four principal seaports. The ports of Veracruz and Altamira are located along the Gulf of Mexico and Lazaro Cardenas and Manzanillo are located on the Pacific coast. Trade at the two Pacific coast ports is growing at an annual rate of approximately 12 percent, partially because U.S. west coast ports are at capacity. Altogether, these four ports account for 92 percent of Mexican maritime trade. Mexico's four major Seaports scan 100 percent of all inbound shipments with VACIS imaging systems. Mexico has implemented a 24-Hour Manifest Rule based upon the U.S. version. The Government of Mexico has the capacity to conduct 100 percent imaging on inbound shipments. Additionally, at the port of Veracruz, the Mexican government installed an integrated scanning lane (a VACIS system integrated with a radiation portal monitor) to scan all exports. Under the Megaports Initiative, Mexico will cost-share with the Department of Energy to install radiation detection equipment to scan all vehicle import and export traffic at each of the four major ports: Veracruz, Altamira, Manzanillo and Lazaro Cardenas.

Canada: Both Canada and the U.S. have signed a Mutual Recognition Arrangement called the Customs-Trade Partnership Against Terrorism (C-TPAT) and Partners in Protection (PIP) agreement, with the goal of securing the entry of goods into the U.S. and Canada by preventing terrorists and their weapons from penetrating the global supply chain.

In addition, the Canada Border Services Agency (CBSA) uses the latest technology to help prevent contraband and dangerous goods from entering Canada by marine trade and other modes of transportation. Such technologies include radiation detection equipment, (VACIS), and Pallet VACIS. The use of these technologies enables CBSA officers to conduct effective, non-intrusive inspections and allows them to focus on high-risk goods.

Mexico: Mexico Customs has deployed 150 handheld radiation detection equipment systems at its seaports and major airports, as well as along the U.S.-Mexico border. Mexico Customs presently runs 69 cargo non-intrusive inspection (NII) equipment sites nationwide scanning rail shipments, empty inbound seaport conveyances and inbound seaport shipments. This equipment includes operational VACIS at the four major seaports. In 2007 the Mexico Ministry of Finance signed a memorandum of understanding (MOU) with the U.S. Department of Energy (DOE) for the implementation of the Megaports Initiative. When fully implemented, this initiative is intended to allow scanning by radiation detection equipment of 100 percent of the imports and exports entering/exiting the port by truck at the four largest Seaports (Veracruz, Manzanillo, Altamira, and Lazaro Cardenas). These four ports handle 92 percent of all seaport cargo. The first Mexican Megaport—Veracruz—is anticipated to be operational in February 2009. Under the MOU, Mexico will share information on detections or seizures of special nuclear and other radioactive materials made as a result of the equipment.

Port	Import	Export	Total
Manzanillo	494,620	425,302	919,922
Veracruz	165,420	243,552	408,972
Lazaro Cardenas	80,654	81,314	161,968
Altamira	107,518	129,587	237,105
Totals	848,212	879,755	1,727,967

United States: U.S. Customs and Border Protection (CBP) has developed numerous programs and systems to identify and select high-risk shipments as part of our multi-layered enforcement strategy. While CBP cannot physically examine all containers, CBP does review virtually 100 percent of all shipments that arrive into the United States. This is accomplished by an electronic review of all shipments through the Automated Targeting System (ATS), which then sorts the shipments by level of risk.

In addition, through the Container Security Initiative, CBP is pushing our nation's zone of security beyond our physical borders by working with nations from around the world to target, screen, and inspect high-risk containers that are bound for the United States.

To further reduce the risk of weapons of mass destruction or illicit nuclear/radiological materials that could be smuggled into the United States, CBP launched the Customs-Trade Partnership Against Terrorism (C-TPAT). As of September 17, 2008, approximately 8,596 certified partners have joined CBP in the war against terrorism. Under the C-TPAT initiative, CBP works with participating companies—i.e., carriers, importers, and other industry sectors—to substantially increase end-to-end supply chain security.

At our land borders, CBP currently deploys multiple technologies to support our multi-layered inspection process. These technologies include large-scale non-intrusive inspection imaging systems, radiation portal monitors, radiation isotope identifier devices and personal radiation detection devices.

Risk assessment and targeting have played an important role in the U.S., Canada and Mexico's commitment to safeguarding North America, as part of the Security and Prosperity Partnership (SPP). At the SPP Montebello Summit in August 2007, the U.S., Canada and Mexico agreed to work together to establish risk-based screening standards for goods and travelers that rely on technology, information sharing and biometrics; develop and implement compatible electronic processes for supply chain security that use advance electronic cargo information to analyze risk and ensure quick and efficient processing at the border; develop standards and options for secure documents to facilitate cross-border travel; and exchange additional law enforcement liaison officers to assist in criminal and security investigations.

Canada: Canada's requirements for the scanning of inbound container cargo are similar to U.S. requirements. The U.S. works closely with Canada under the Container Security Initiative (CSI) to detect and deter terrorist use of maritime containers while facilitating the movement of legitimate trade. CBP officers have been assigned to three major ports of entry in Canada—Halifax, Vancouver and Montreal—to screen manifest data before a container is shipped to the U.S. by cross-referencing CBP data bases. Canadian host government officers will then examine containers which pose a potential risk to the U.S., using either radiation detectors or large-scale radiographic imaging machines to detect potential terrorist weapons. Similarly, Canadian joint task officers under the SPP agreement are stationed in Newark and Seattle to perform functions similar to those that CBP CSI officers perform in Canada, in an effort to increase security for containerized cargo destined to Canada.

Mexico: Mexico has scanning requirements in place and strives to mirror those of the U.S., but has less experience in conducting risk assessment. Mexico Customs is in the process of establishing its own National Targeting Center (NTC) similar to the one CBP currently has. CBP will play a key role in assisting Mexico Customs to stand up its operations and then to develop targeting systems modeled after the CBP systems.

Question 5. At present, do cargo containers unloaded off ships in Canadian and Mexican ports get transshipped by rail and truck to final destinations in the United States?

Currently, what is the level of cooperation and coordination between U.S. and Canadian authorities and U.S. and Mexican authorities to ensure that these transshipped U.S.-bound cargo containers do not present a significant risk for weapons of mass destruction?

Does Customs and Border Protection need additional authority in this area, for example with respect to international freight rail crossing at the U.S. border?

Answer. There are many trade lanes available which an importer may utilize while importing cargo into the United States. Transshipping cargo by rail/truck from Mexico or Canada is a viable option that is routinely used. Approximately 98 percent of all containers entering the United States from Mexico or Canada are scanned by a RPM device upon entry regardless of their country of origin.

Seaport security programs in place in Mexico and Canada provide an additional layer of screening and scanning of transshipped cargo. As was discussed above, 92 percent of Mexican maritime trade arrives at one of four principal ports. The Government of Mexico already has 100 percent imaging capacity for inbound shipments and, under the Megaports Initiative, is cost-sharing with the Department of Energy to install radiation detection equipment to scan all exports and imports arriving/departing by truck at each of its four major ports. Under a pilot program, Mexico installed an integrated scanning lane (a VACIS co-located with a radiation portal monitor) at the Port of Veracruz to scan all exports.

CBP has the authority to examine all cargo entering the United States, regardless of mode.

Question 6. As you know, in 2012, there is a 100 percent scanning requirement for U.S.-board cargo containers. Will the 100 percent scanning requirement apply

to cargo containers destined for Canada and Mexico ports which are subsequently transshipped by truck and rail to the United States?

If it doesn't apply, are we creating a loophole that could potentially be exploited by bad actors? If it does apply, would the scanning have to be performed in Canadian and Mexican ports?

Answer. Section 1701 of the 9/11 Act (H.R. 1, 110th Congress) amended the SAFE Port Act and charges DHS with achieving full-scale implementation of overseas scanning by July 1, 2012, but permits extensions by certifying to Congress that at least two of the six conditions outlined in Section 1701(b)(4) apply. The 9/11 Act changed the dynamic of the ongoing pilot programs from exploring the feasibility of overseas scanning to developing real, practical solutions to meet the challenges that arise. These challenges continue to be significant. The extensions permitted under the law recognize some of the difficulties that may occur in developing an overseas scanning strategy, including the impact on trade capacity and the flow of cargo, whether the systems can be integrated with existing systems, and the infrastructure restraints of foreign ports. We continue to refine and develop our expansion approach as we move toward the initial 2012 deadline.

We do not believe any loophole exists with transshipped containers from Mexico or Canada. Approximately 98 percent of all containers entering the United States across our land borders are currently scanned by a RPM device regardless of their original country of origin. We continue working with our partners in Canada and Mexico to provide additional layers of security at their seaports as well as at our land points of entry (POE). In fact, under the Megaports Initiative, DOE is working with Mexico to equip all four of its major seaports with radiation detection equipment in order to scan all import and export traffic arriving/departing Mexico by truck.

Question 7. There has been considerable concern in Congress about the performance capabilities of Advanced Spectroscopic Portal Monitors (ASP's) and the FY 2007 DHS Appropriations Act required the Secretary of DHS to certify a significant increase in operational effectiveness prior to moving forward with the Administration's proposal for full scale deployment. Has Secretary Chertoff concluded the additional testing of the ASP's and provided his certification to Congress? Was the technology tested in the SFI pilot? If yes, what was the performance findings of the technology?

Answer. The ASP is currently undergoing integration testing at Pacific Northwest National Laboratories (PNNL). During this integration period, the ASP is tested in a mock CBP Port of Entry (POE) to ensure that the ASP can operate properly with all of CBPs ancillary systems (*i.e.*, traffic control mechanisms, stop lights, gate arms, etc.). Upon successful completion of this testing, CBP will conduct a field validation of the ASP in four high volume POEs; Long Beach, CA, New York Container Terminal, Detroit, MI, and Laredo, TX. This validation test will be conducted in the stream of commerce at the Northern land border, Southern land border and seaport environments to ensure the ASP is robust enough to operate at CBPs POEs. Upon successful completion of this test and validation, CBP, jointly with the Domestic Nuclear Detection Office (DNDO), will recommend certification by the Secretary of the Department of Homeland Security.

The ASP is currently being tested in the SFI port of Southampton, U.K. The Department of Energy (DOE) has purchased a limited number of ASP detection devices and deployed a unit at Southampton as part of an ongoing effort to gain both operational experience and insight into the viability of these units as radiation detection/isotope identification devices in a secondary application. The ASP is undergoing a DOE field test and is not used for official adjudication of RPM alarms. If a U.S. bound container generates a radiation alarm at an RPM, it is subsequently scanned both by the ASP and by a handheld ORTEC (a radioisotope identification device). The DOE and DNDO are evaluating the robustness of the ASP, as well as the data transmitted to the United States.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK. R. LAUTENBERG TO
DAVID HUIZENG

Question 1. In your testimony you state that NNSA has installed over 1,000 RPMs at over 160 sites. Are you procuring and installing equipment that conforms to the technology performance standards that the United States has set for domestic scanning equipment?

Answer. DOE and DHS have very similar performance standards for radiation portal monitors (RPMs). The primary difference is that the DOE standards are defined in terms of quantities of Special Nuclear Material (SNM) while DHS standards

are defined in terms of surrogate materials. The advantage of defining standards in terms of surrogate materials is that these materials are available commercially and RPM vendors can evaluate their monitors on their own. The disadvantage of the surrogate materials is there are some slight differences in the radiation characteristics compared to the SNM they represent. However, the differences between the standards have been thoroughly evaluated by DOE and DHS technical staff and are believed to be minor when evaluating monitor performance.

Question 2. In your testimony you state that the goal of the Megaports Initiative is to equip approximately 75 priority ports with scanning technology by 2013, at which point you estimate that you will be scanning over 50 percent of global shipping traffic. Does this just cover the radiological detection equipments such as RPM or would this also include the non-intrusive imaging equipment such as VACIS? What specific equipment are we talking about here? What do you estimate the cost to be to the U.S. Government to achieve this goal? What do you estimate the cost to be to our trading partners? How many international trade agreements will you have to negotiate to achieve this goal?

Answer. The mission of DOE's Megaports Initiative is to provide partner nations with passive radiation detection equipment (*i.e.*, radiation portal monitors (RPMs and handheld detection equipment), communications and training and technical support to enhance their capacity to deter, detect, and interdict illicit trafficking of special nuclear and other radioactive materials through the global maritime system. DOE does not provide partner nations with non-intrusive imaging equipment.

DOE's budget request from FY 09 through FY 13 is \$818 million and supports the installation of radiation detection equipment at a total of 75 Megaports. The Megaports Initiative is also working with partner nations to develop cost-sharing agreements. To date, we have agreed to cost-sharing agreements for ports in Honduras, Israel (two), Colombia, Panama (multiple), Mexico (multiple), Belgium and Spain (two). Cost-sharing is a high priority for us and estimates on number of ports that will cost-share have been and will continue to be incorporated into our budget planning and requests.

With regard to anticipated costs to our trading partners, one of the top priorities of the Megaports Initiative is to install our equipment in a manner that will not interrupt the normal flow of containers through a port and thus increase costs. When designing an installation, the Megaports Initiative looks to place monitors at natural chokepoints, such as entry and exit gates, so that containers are scanned without deviating from their normal route. For container traffic that does not move through the gates, such as transshipped containers, DOE has deployed several new mobile technologies, including a radiation detection straddle carrier and a Mobile Radiation Detection and Identification System (MDRIS). DOE is also active in following and evaluating new technologies closely to determine any areas where improvements in scanning may be made.

Our partner countries are responsible for staffing the radiation monitoring systems. In addition, after an initial period when maintenance costs for the deployment are provided by DOE, the partner country assumes the cost of maintaining and sustaining the equipment. These costs vary significantly in terms of the number of monitors deployed and the labor rates within a country. To date, the average annual cost of a maintenance contract has been approximately 88K USD annually and it is assumed the partner country will incur similar costs when it takes over the maintenance responsibility. The amount of additional work, and hence the staffing load that a radiation detection system brings to a port is dependent on several factors. In some cases, existing staff can easily absorb the amount of additional work. In other cases, additional personnel are required, perhaps dedicated fully to operating the SLD-provided equipment. The impact on staffing is estimated based on operational factors such as number of lanes with installed radiation detection equipment, amount of traffic, and expected number of innocent alarms.

DOE has not been involved in any international trade agreements with regard to the installation of radiation detection equipment. Typically, DOE signs a Memorandum of Understanding (MOU) or a Declaration of Principles (DoP) with partner nations to implement the Megaports Initiative. However, DOE has also pursued other arrangements, such as letters of exchange or joint press releases, with Pakistan, Hong Kong, Japan, and the United Kingdom. To date, DOE has signed 24 agreements (MOUs or DoPs) and issued the aforementioned four additional agreements, representing work commitments at more than 40 seaports around the world. DOE will continue outreach efforts to negotiate additional agreements and meet the goal of 75 operational ports by 2013.

Question 3. Is DOE conducting its own testing of the ASP's at the Nevada Test Site and if so, why? Has DOE purchased or is it planning to purchase any ASP's

and if so where will they be deployed? How many have been purchased? Why would DOE purchase any before the second round of testing is complete and the Secretary of DHS has certified to the ASP's effectiveness?

Answer. DOE has been working closely with DNDO to comprehensively test the ASP. Specifically, we have participated in Technical Summits to establish the path forward for the ASP program, conducted a significant data collection effort at Los Alamos National Laboratory using special nuclear materials, provided technical experts to perform data analysis during the current data collection at the Nevada Test Site, and will continue providing input into future test plans and the injection studies.

In addition to these activities, DOE has conducted some of its own testing of the Thermo Fisher ASP at the Los Alamos National Laboratory (LANL). The scope of this testing is to define the concept of operations that may be suitable for secondary screening at international seaports. The scope of the testing is not intended to duplicate the performance testing being conducted by DNDO but to supplement DOE's understanding of how best to deploy the equipment.

DOE's Megaports Initiative purchased 12 ASPs from Thermo Fisher through a DNDO contract in 2006. Due to the potential advantages for more efficient cargo screening, DOE decided to purchase a limited number of ASPs to evaluate their performance in operational settings for secondary inspections. DOE has deployed these units for secondary inspections both to operational Megaports (Southampton, U.K. and Antwerp, Belgium) and to the laboratories to gather further data of the ASPs performance in a variety of settings. Additional units are planned for installation at Colombo, Sri Lanka, and Manila, Philippines, Kaohsiung, Taiwan and Port Klang, Malaysia. These systems are currently operated in tandem with existing secondary screening protocols, including inspection with handheld radiation isotope identification devices, until the ASPs have been shown to operate reliably and effectively in the field.

Overall, DOE has been closely involved in the testing conducted with DNDO on the ASP and has developed its own test plans to further evaluate the performance of the ASP. The testing completed by the labs combined with the data we are receiving from our operational testing and evaluation of the ASP units we have in the field will provide valuable technical and operational insight for future deployments. As we move forward with testing and evaluation, it is our expectation that we will continue to work closely with our DHS counterparts.

Question 4. I was interested to read about the technology you are testing for mobile radiological detection platforms on straddle carriers in the Bahamas. You indicate that over 730,000 containers have been successfully scanned. Over what time period is that metric based? Has this technology performed well? And, again, just to clarify, that is only a radiological scan, not an NII?

Answer. Yes, the radiation detection straddle carrier (RDSC) deployed in the Bahamas only scans containers for radiation and does not have a non-intrusive imaging component. The Megaports Initiative deployed a prototype RDSC to the Bahamas in 2005 for testing. This unit became officially operational in June 2006. This unit was designed specifically to address the configuration of the Port of Freeport, which exclusively uses straddle carriers for moving and stacking cargo containers, up to three high, around the lay-down yard in rows. To address this terminal configuration, the Megaports Initiative modified one standard straddle carrier by stripping it of its lifting mechanisms and equipping it with both portal monitors, which detect the presence of radiation, and spectroscopic detectors, which can identify the source of radiation causing an alarm. The RDSC traverses container rows, scanning containers stacked in the lay-down yard. The unit is also equipped with a global positioning system (GPS) and a wireless communications system to give precise location data and to transmit information generated from scan to a Central Alarm Station (CAS) where alarms are assessed and adjudicated by Bahamian Customs Officers.

The unit has performed very well with over 800,000 containers scanned at the Port of Freeport from June 2006 through August 2008. On average, the straddle carrier has scanned approximately 85 percent of containers passing through Freeport. The RDSC has also demonstrated one solution to the challenge of transshipment containers (*i.e.*, those containers that move from one ship to another without every passing through an entry or exit gate) faced by the Megaports Initiative, by allowing containers to be scanned in the lay-down yard as they await movement to their next destination. Based on the success of the RDSC, DOE has recently awarded a commercial contract for the design and manufacture of additional straddle carrier units, which will be deployed to other straddle carrier ports in the future. The initial RDSC produced under the new contract is expected to undergo acceptance testing in late FY 2009.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
STEPHEN L. CALDWELL

Question 1. What are the national policies of Canada and Mexico with respect to scanning of inbound cargo containers? Does either Canada or Mexico have scanning requirements to prevent weapons of mass destruction from entering their ports of entry in cargo containers? If either nation does have such a requirement, is it stronger or weaker than the U.S. requirements for the scanning of inbound container cargo?

Answer. While GAO has not performed audit work examining the national policies of Canada or Mexico with respect to the scanning of inbound cargo containers, or reviewed whether their requirements are stronger or weaker than those of the United States, we have some information on Canada Border Services Agency (CBSA) efforts to prevent weapons of mass destruction from entering Canada.

Canada employs a risk-management system for identifying high-risk container cargo bound for Canadian seaports. In particular, CBSA receives advanced information for all marine vessels destined to arrive at ports in Canada and uses a system which generates a risk score. This risk score is then forwarded to Canadian targeters for review. Marine vessel targeting is divided by risk level, with the National Risk Assessment Center (which CBSA officials describe as being similar to the U.S. National Targeting Center) looking for threats for national security (e.g., weapons of mass destruction and radioactive materials). Regional targeters focus on contraband, environmental contaminants (e.g., pine beetles, chemicals, etc.) and other threats. NRAC targeters review risk scores for each shipment and conduct an in-depth assessment of the shipments identified as posing a potential national security threat. If the CBSA officers identify a suspicious shipment, they may issue a “do not load” or “do not unload” order and the cargo is examined either in a foreign port or upon arrival depending on the nature of the threat.

The Canadian government has also initiated the Partners-in-Protection (PIP) program to enlist the cooperation of companies involved in interational commerce in enhancing border security, combating terrorism, and helping to detect and prevent contraband smuggling. Participating companies sign a Memorandum of Understanding with CBSA, which focuses on the security of the trading companies’ cross-border operations (particularly the security of its supply chain), information exchanges, and joint training activities. This program is similar to the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) program. Additionally, since 2001, the Canadian government has deployed new inspection equipment, such as Vehicle and Cargo Inspection System (VACIS) machines and x-ray scan trailers. In a 2005 report, CBSA anticipated that it would have the capacity to conduct radiation checks on almost all marine containers arriving at the ports of St. John, Halifax, Montreal and Vancouver which together receive nearly all container traffic arriving at Canada’s marine ports of entry.

Question 2. At present, do cargo containers unloaded off ships in Canadian and Mexican ports, get transshipped by rail and truck to final destinations in the United States? Currently, what is the level of cooperation and coordination between U.S. and Canadian authorities and U.S. and Mexican authorities to ensure that these transshipped U.S.-bound cargo containers do not present a significant risk for weapons of mass destruction? Do Customs and Border Protection and NMSA need additional authority in this area, for example with respect to international freight rail crossing at the U.S. border?

Answer. While GAO has not reviewed cargo container operations at Mexican seaports, based on prior audit work we know that some container cargo arriving at Canadian seaports is transported to the United States. For example, on a visit to the Port of Halifax, Nova Scotia in 2006, CBSA officials told us that a portion of the container cargo arriving at the port is loaded on to trains for delivery to the United States. Regarding coordination efforts to ensure that this cargo bound for the United States does not pose a security risk, U.S. Customs and Border Protection (CBP) deploys targeters to ports in Vancouver, Montreal, and Halifax as part of the Container Security Initiative (CSI). These targeters review automated targeting system (ATS) information and work with CBSA officials to identify containers that may pose a security risk. Similarly, Canadian targeters located at the ports in Newark and Seattle review marine containers arriving at U.S. ports destined for Canada by rail or by truck. At these U.S. seaports, CBP officials assess all shipments for national security threats, while Canadian targeters concentrate on identifying contraband smuggling. If the Canadian targeters wish to refer a container for examination, they submit a formal request to U.S. authorities to conduct the examination at the port of entry.

GAO has not performed any audit work regarding the issue of whether CBP and NMSA need additional authority regarding transshipped rail cargo bound for the United States. We leave it up to those respective agencies to comment on whether they believe their current authority is sufficient.

Question 3. As you know, in 2012 there is 100 percent scanning requirement for U.S.-bound cargo containers. Will the 100 percent scanning requirement apply to cargo containers destined for Canada and Mexico ports which are subsequently transshipped by truck and rail to the United States? If it doesn't apply, are we creating a loophole that could potentially be exploited by bad actors? If it does apply, would the scanning have to be performed in Canadian and Mexican ports?

Answer. The statutory requirement for 100 percent scanning does not expressly include or exclude cargo containers destined for Canadian or Mexican ports which are subsequently transshipped by truck or rail to the United States.¹ In our audit work to date, we have not obtained an official position from CBP as to whether it intends to apply the 100 percent scanning requirements to such cargo containers. As our audit work continues, we will continue to seek an official position from CBP.

This issue is particularly important since Canada has recently expanded some of its seaports with the intent to then ship containers into the United States over land borders. These include the expansion of the seaport in Vancouver and the building of a new container terminal in Prince Rupert at a cost of approximately one billion U.S. dollars. However, CBP does receive advanced information for cargo that arrives in Canada via ship and is then transported to the United States via rail. Two rail carriers, CN and CP, carry such containers to the United States and both are C-TPAT approved carriers. Rail carriers transmit electronic data to CBP 2 hours in advance of the cargo's arrival at the U.S./Canadian border. CBP officers assess the cargo data and determine whether a threat exists. If they determine it is a risk or threat, they will place a "hold" on the container for the carrier with instructions to "set out" the container for examination. When the train arrives at the border, CBP conducts VACIS inspection of all cars on the train.



¹See Section 1701(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110-53, § 1701(a), 121 Stat. 266,489-90).