

**THE SAFE PORT ACT: STATUS OF
IMPLEMENTATION ONE YEAR LATER**

HEARING

BEFORE THE

**SUBCOMMITTEE ON BORDER, MARITIME,
AND GLOBAL COUNTERTERRORISM**

OF THE

**COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES**

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 30, 2007

Serial No. 110-80

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpoaccess.gov/congress/index.html>

U.S. GOVERNMENT PRINTING OFFICE

48-975 PDF

WASHINGTON : 2009

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DeFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of
Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin
Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. McCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*

ROSALINE COHEN, *Chief Counsel*

MICHAEL TWINCHEK, *Chief Clerk*

ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL
COUNTERTERRORISM

LORETTA SANCHEZ, California, *Chairwoman*

JANE HARMAN, California
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
AL GREEN, Texas
BENNIE G. THOMPSON, Mississippi (*Ex
Officio*)

MARK E. SOUDER, Indiana
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. McCAUL, Texas
GUS M. BILIRAKIS, Florida
PETER T. KING, New York (*Ex Officio*)

ALISON ROSSO, *Director*

DENISE KREPP, *Counsel*

CARLA ZAMUDIO-DOLAN, *Clerk*

MANDY BOWERS, *Minority Senior Professional Staff Member*

(II)

CONTENTS

	Page
STATEMENTS	
The Honorable Loretta Sanchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Border, Maritime, and Global Counterterrorism:	
Oral Statement	1
Prepared Statement	2
The Honorable Mark E. Souder, a Representative in Congress from the State of Indiana, a Ranking Member, Subcommittee on Border, Maritime, and Global Counterterrorism	3
The Honorable Bennie G. Thompson, a Representative in Congress from the State of Mississippi, and Chairman, Committee on Homeland Security:	
Oral Statement	4
Prepared Statement	5
The Honorable Gus M. Bilirakis, a Representative in Congress from the State of Florida	39
The Honorable Henry Cuellar, Representative in Congress from the State of Texas	44
The Honorable Al Green, a Representative in Congress from the State of Texas	40
The Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas	42
The Honorable Daniel E. Lungren, a Representative in Congress from the State of California	3
The Honorable Michael T. McCaul, a Representative in Congress from the State of Texas	83
The Honorable Bill Pascrell, Jr., a Representative in Congress from the State of New Jersey	45
WITNESSES	
PANEL I	
Mr. Stephen L. Caldwell, Director, Homeland Security and Justice Issues, Government Accountability Office	32
Ms. Maurine Fanguy, Program Director, Transportation Security Administration, Department of Homeland Security:	
Oral Statement	7
Prepared Statement	8
Mr. Vayl Oxford, Director, Domestic Nuclear Detection Office, Department of Homeland Security:	
Oral Statement	28
Prepared Statement	30
Captain Francis Sturm, U.S. Coast Guard, Department of Homeland Security:	
Oral Statement	11
Prepared Statement	13

IV

	Page
Mr. Thomas Winkowski, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security:	
Oral Statement	21
Prepared Statement	23

PANEL II

Ms. Mary Alexander, Chair, Joint Industry Group:	
Oral Statement	67
Prepared Statement	69
Mr. Wade Battles, Managing Director, Port of Houston Authority:	
Oral Statement	73
Prepared Statement	74
Mr. Robert F. Blanchet, Teamster Port Representative, International Brotherhood of Treamsters:	
Oral Statement	53
Prepared Statement	55
Mr. Christopher Koch, President, World Shipping Council:	
Oral Statement	58
Prepared Statement	59
Mr. Lindsay McLaughlin, Legislative Director, International Longshore and Warehouse Union:	
Oral Statement	49
Prepared Statement	51

APPENDIXES

A: Executive Summary of C-TPAT Partners Cost-Benefit Survey Prepared by the University of Virginia for U.S. Customs and Border Protection	87
B: Additional Questions and Responses	
Panel I	
Responses from:	
Mr. Stephen L. Caldwell	91
Ms. Maurine Fanguy	95
Mr. Vayl Oxford	97
Captain Francis Sturm	100
Mr. Thomas Winkowski	106
Panel II	
Responses from:	
Ms. Mary Alexander	116
Mr. Wade Battles	120
Mr. Robert F. Blanchet	124
Mr. Christopher Koch Responses	126

THE SAFE PORT ACT: STATUS OF IMPLEMENTATION ONE YEAR LATER

Tuesday, October 30, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER, MARITIME,
AND GLOBAL COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to call, at 2:17 p.m., in Room 311, Longworth House Office Building, Hon. Loretta Sanchez [chairwoman of the subcommittee] presiding.

Present: Representatives Sanchez, Jackson Lee, Langevin, Green, Thompson (Ex Officio), Souder, McCaul, Bilirakis, and King (Ex Officio).

Also Present: Representative Lungren.

Ms. SANCHEZ. The Subcommittee on Border, Maritime and Global Counterterrorism will come to order. And the subcommittee is meeting today to receive testimony on the SAFE Port Act Status of Implementation One Year Later.

I would, at this time, ask unanimous consent that Mr. Lungren of California be allowed to sit and question at today's hearing. No hearing no objection, welcome, Mr. Lungren. Always great to have a fellow Californian on.

Thank you to our witnesses for joining us today, particularly since this hearing was postponed from earlier in the month. And I appreciate your flexibility in coming before our committee again.

Today we will be discussing the status of the implementation of the SAFE Port Act, as you know, one of the pieces of legislation from the 109th Congress that I think is probably one of the most important we passed. And, of course, we passed it on the last day of that Congress. The legislation was a cumulation of years of work by many on this committee and other Members of Congress, and I do believe that once it is implemented, it will improve the security of our Nation's ports. And as a member of a district who lives 20 minutes away from the largest port system in the United States, that is Long Beach-Los Angeles, it is incredibly important to me personally and to the people that I represent.

So, it is our intention, and certainly my intention that we implement this and we oversee it and we get it done as quickly as possible. As you know, we have already held a 6-month hearing on the SAFE Port Act, and here we are 6 months later wanting to know what has been going on.

I hope that today's hearing will update us on many of the initiatives. I have several that I am particularly interested in. You all

probably already know, but just in case, an explanation of the aspects of C-TPAT's third-party verification program, the pilot, and the update on its progress, the status of the empty security pilot program that was required by the law, the Coast Guard's long-range vessel tracking capability, and their ability to view that data in a usable format; and of course, the delayed progress on the Transportation Worker Identification Credential, or the TWIC.

And I hope that our witnesses will address these items as well as many of the others that need to be addressed as to what is going on with the SAFE Port Act. And I am pleased to hear that the agencies within the Department are making progress on some of these provisions, but we want to make sure you are making progress as quickly, as safely as possible.

Some of my concerns also include the establishment of the container security standards and improvements to CBP's risk targeting, a lack of the fully operational vessel tracking system to tell us what vessels are coming to American ports, and of course, the efficient rollout of the TWIC program that would ensure that our ports are safe without compromising American jobs or adding excessive costs.

And I would like to thank my ranking member, Mr. Souder, for his interest in this important issue, and at this moment I would like to recognize the ranking member of the subcommittee, the gentleman from Indiana, for his opening statement.

PREPARED STATEMENT OF THE HONORABLE LORETTA SANCHEZ, CHAIRWOMAN,
SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

Good Afternoon.

Thank you to our witnesses for joining us today, particularly since this hearing was postponed from earlier in the month. We appreciate your flexibility.

Today we will be discussing the status of implementing the SAFE Port act, over one year after it became law.

This Subcommittee held a similar hearing six months ago and I know my colleagues and I are eager for an update on the Government's progress.

I believe that the SAFE Port Act was one of the Homeland Security Committee's most significant actions of the 109th Congress.

This legislation was the culmination of years of work by numerous Members of Congress, and it made long overdue improvements to the security of our nation's ports.

As a Member whose district is close to the Los Angeles and Long Beach Ports, I am very aware of the direct impact port security has on the lives and livelihoods of all Americans.

I intend to make sure that the 110th Congress conducts appropriate oversight to ensure that the SAFE Port Act is fully implemented.

As we all know, the SAFE Port Act covered a wide range of programs and initiatives at the Department of Homeland Security.

I hope that today's hearing will provide us with an update on these many initiatives.

There are several issues that I am particularly interested in.

These include:

- An explanation of aspects of the C-TPAT 3rd party validator pilot program and an update on its progress;
- The status of the empty container security pilot program required by the law;
- The Coast Guard's long range vessel tracking capability and their ability to view that data in a useable format;
- AND, or course the delayed progress on the Transportation Work Identification Credential, or TWIC.

I hope our witnesses will address these items among many other critical issues in the SAFE Port act.

I am pleased to hear that the agencies within the Department are making progress on some of the provisions in the SAFE Act, but we must ensure that the law is fully implemented so our ports are as secure as possible.

Some of my concerns include:

- The establishment of container security standards and improvements to CBP's risk targeting;
- The lack of a fully operational vessel tracking system to tell us what vessels are coming to American ports;
- AND the efficient roll out of a TWIC program that ensures the security of our ports without compromising American jobs, or adding excessive costs.

I'd like to thank my ranking Member, Mr. Souder for his interest in this important issue.

Mr. SOUDER. Thank you very much, Madam Chair. And we are 1 year out from the enactment of the SAFE Port Act and 6 months from the implementation status. Like with other areas of homeland security, there is no silver bullets. Securing maritime transportation system from the beginning of the supply chain through the arrival at U.S. ports and delivery, requires overseas cooperation, participation from the private sector, technology, resources and intelligence.

In many ways, defending against terrorists is similar to detecting and disrupting illegal narcotics. Step one, stop the terrorist activity and plans in the source country. Step two, prevent weapons and terrorists from exiting the source country for the United States. Step three, interdict the illicit activity en route. Step four, stop it at the port of entry or along the border in coastal areas. Five, detect movement within the United States. And, six, address the threats on the streets of our towns and cities.

Addressing these steps requires a layered security strategy. The one absolute about terrorists is that they strive to be unpredictable. To counter this, we have to have some level of uncertainty in our security response and robust layers of security throughout the supply chain. Ultimately, intelligence is our best weapon. It is not possible to do everything all the time. We have to have some odds projection inherent in our security measures. We also have to be constantly changing our pattern so that terrorists are lost at sea when it comes to learning and exploiting our vulnerabilities. This enhances the deterrent factor.

I look forward to the testimony today and to hearing what progress has been made implementing the SAFE Port Act and where we are lacking. According to the committee Republican staff report that reviewed the Department's efforts over the past year, DHS has made substantial progress in many areas. The secure freight initiative stands out as one where DHS is ahead of schedule in implementing the 100 percent inspection pilots in complete accordance with the laws so far.

In other areas, there is clearly more work to do. TWIC, setting standards for securing containers, and enhancing the high-risk targeting system are several areas where I am looking forward to hearing from our witnesses.

That will complete my statement, and I would like to yield the rest of my time to Congressman Lungren who was the sponsor of the SAFE Port Act and is a member of the full committee.

Mr. LUNGREN. I thank the gentleman for yielding. I thank the Chairlady for allowing me to participate in this hearing today. I will have to leave at one point in time to represent our side in the

defense authorization conference on behalf of the Homeland Security Committee, but I share the gentlelady's appreciation for the tremendous positive impact that the ports of Long Beach and L.A. have, not only in California, but throughout the country and the importance of this bill.

There is, of course, no perfect bill, there is no perfect law, and there is no perfect implementation. But I think we can take tremendous pride in the fact that we delivered a good bill that was signed into law by the President and that, based on our staff's review of this and based on GAO's review of this, that by and large, this has been implemented well under all circumstances that would be considered.

We can always do better. But I think it is an important message for us to give the American people that they are safer as a result of the actions that have been taken by this Congress in cooperation with the administration since 9/11, and specifically since October 13 of last year when the President signed H.R. 4954, the SAFE Port Act, we have moved forward. And I look forward to hearing the testimony here, the details, and also what more we might be able to do to assist in further implementation. And I thank the gentlelady.

Ms. SANCHEZ. The Chair will now recognize the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Madam Chairman. I am happy to be here for this hearing. It has been a year since the SAFE Port Act was signed into law, and we are here today to learn about the Department of Homeland Security's implementation of this important Act.

Maritime security is a paramount importance to the United States. 95 percent of the goods destined for the United States arrive in our Nation's seaports. These seaports and the men and women who work on these ports must be protected. Unfortunately, the Department of Homeland Security is not protecting these men and women to the extent it should. The Department of Homeland Security, plagued with a lack of leadership, is allowing these men and women to remain at risk. We owe the American people security. We owe them accountability. And, most importantly, we owe them freedom from fear.

We are here today to find out why the Department of Homeland Security has failed in its mission to improve the maritime security. The Department of Homeland Security's failure to implement the Transportation Worker Identification Credential is a perfect example of this failure. The Department began rolling out the TWIC program, which was mandated 5 years ago. just 2 weeks ago. Already, there are glaring problems. The Department significantly underestimated the number of workers who are required to get a TWIC. The Department estimated that 30,000 workers would need to get a TWIC card in the Port of Houston. According to the Port of Houston, the real number is closer to 350,000. At the Port of New York and New Jersey, the Department again underestimated the number. The Department's estimate was 60,256. The real number is closer to 125,000.

The Department's inability to successfully project the correct number of workers is compounded by the fact that the TWIC readers are years away from installation. Without the readers, a TWIC is merely a flash pass that can be fraudulently duplicated and misused. This misuse has already begun. Last week, the Coast Guard, issued an advisory stating that criminal elements were trying to obtain information about the TWIC program at the ports of Los Angeles and Long Beach.

Five years and millions of dollars later, this program has already been compromised. The potential compromise is shocking, considering the fact that the Department has only rolled out the TWIC at one port. The Department provided the list today of its tentative rollout schedule for the rest of the ports.

As in the past, the list does not contain concrete information; it contains vague dates. Vague dates are not good enough. Our ports should be given specific information to enable them to successfully roll out the TWIC at their ports.

Unfortunately, TWIC is not the Department's only troubled program. The Department has failed to develop a container security device regulation required by the SAFE Port Act. The Department claims that the technology does not exist. It does, and I have one that I would like to show to Customs and Border Protection here today. This device is made by General Electric. Other companies have developed their own versions. So it does exist. The Department's failure to develop the regulation is just another example of the Department's unwillingness or inability to follow the mandates clearly laid out by Congress. We established these mandates because we are committed to improving our Nation's maritime security. We specifically told the Department to develop a strategic plan to enhance the security of the international supply chain. The Department did not develop a plan; it developed yet another document that will sit on the shelf collecting dust.

Philip Spayd, in an August 27, 2007 article in the Journal of Commerce, summed it up best: The 128-page plan would receive a high grade as a research project for a graduate school class in international logistics, but which lacks any operational grounding.

It is time for the Department to develop this operational grounding, and it is time for the Department to meet the mandate set by the American public, freedom from fear.

PREPARED STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY

ood morning and thank you for being here today.

It has been a year since the SAFE Port Act was signed into law, and we are here today to learn about the Department of Homeland Security's implementation of this important Act.

Maritime security is of paramount importance to the United States. Ninety-five percent of the goods destined for the United States arrive at our nation's seaports. These seaports and the men and women who work on these ports must be protected.

Unfortunately, the Department of Homeland Security is not protecting these men and women to the extent it should. The Department of Homeland Security, plagued with a lack of leadership, is allowing these men and women to remain at risk.

We owe the American people security. We owe them accountability. And most importantly, we owe them freedom from fear. We are here today to find out why the Department of Homeland Security has failed in its mission to improve the maritime security.

The Department of Homeland Security's failure to implement the Transportation Worker Identification Credential (TWIC) is a perfect example of this failure. The Department began rolling out the TWIC program, which was mandated five years ago, just two weeks ago.

Already there are glaring problems. The Department significantly underestimated the number of workers who are required to get a TWIC. The Department estimated that 30,000 workers would need to get a TWIC in the Port of Houston. According to the Port of Houston, the real number is closer to 350,000. At the Port of New York and New Jersey, the Department again underestimated the number. The Department's estimate was 60,256. The REAL number is closer to 125,000.

The Department's inability to successfully project the correct number of workers is compounded by the fact that the TWIC readers are years away from installation. Without the readers, a TWIC is merely a flash pass that can be fraudulently duplicated and misused. This misuse has already begun. Last week, the Coast Guard released an advisory stating that criminal elements were trying to obtain information about the TWIC program at the Ports of Los Angeles and Long Beach. Five years and millions of dollars later, this program may already be compromised.

The potential compromise is shocking considering the fact that the Department has only rolled out the TWIC at one port. The Department provided a list today of its tentative rollout schedule for the rest of the ports.

As in the past, this list does not contain concrete information—it contains vague dates.

Vague dates are not good enough—our ports should be given specific information to enable them to successfully roll out the TWIC at their ports.

Unfortunately, TWIC is not the Department's only troubled program. The Department has failed to develop the container security device regulation required by the SAFE Port Act. The Department claims that the technology does not exist. It does and I have one that I would like to show to Customs and Border Protection today. This device is made by General Electric and other companies have developed their own versions. The Department's failure to develop the regulation is just another example of the Department's unwillingness or inability to follow the mandates clearly laid out by Congress.

We established these mandates because we are committed to improving our nation's maritime security. We specifically told the Department to develop a Strategic Plan to Enhance the Security of the International Supply Chain. The Department did not develop a plan; it developed yet another document that will sit on the shelf collecting dust.

Philip Spayd in an August 27, 2007 article in the Journal of Commerce sums it up best the "128-page plan would receive a high grade as a research project for a graduate school class in international logistics, but which lacks any operational grounding."

It is time for the Department to develop this operational grounding and it time for the Department to meet the mandate set by the American public—freedom from fear.

Ms. SANCHEZ. Other members of the subcommittee are reminded that, under the committee rules, opening statements may be submitted for the record.

I welcome our first panel of witnesses. I will go through your backgrounds a bit, and then we will start from my left through the right for 5 minutes apiece, or under, if you can do that, to summarize your testimony.

Our first witness, Ms. Maurine Fanguy, is director of the Transportation Worker Identification Credential, the TWIC program, at the Transportation Security Administration. And prior to joining TSA, she provided business and technology consulting services to private and public sector clients. She also worked on a wide range of homeland security-related projects there, including border management issues and the application of biometric technologies.

Our second witness is Captain Francis Sturm, Deputy Director For Prevention Policy under the Assistant Commandant For Marine Safety, Security, and Stewardship at U.S. Coast Guard Headquarters. In this position, which he has held since May of 2006, Captain Sturm establishes and coordinates policies and priorities

for inspection and compliance field missions. He previously served as chief office of port and facility activities at Coast Guard Headquarters from August of 2004.

Our third witness is Mr. Winkowski, Assistant Commissioner for the Office of Field Operations at U.S. Customs and Border Protection. In that position, which he has held since August, he manages an operating budget approaching \$2.5 billion, directs the activities of 24,000 employees, and oversees programs and operations at 20 major field offices, 326 ports of entry, 58 operational container security initiatives ports, and 15 pre-clearance stations in Canada, Ireland, and the Caribbean. Thank you for making the time to be here with all that.

Our fourth witness is Mr. Vayl Oxford, director of the Domestic Nuclear Detection Office at the Department of Homeland Security. Mr. Oxford was appointed director in December of 2006. He is responsible for DNDO's jointly staffed office which serves as the primary entity in the United States Government to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation and to further enhance this capability over time. Welcome.

And our final witness on the first panel is Mr. Stephen L. Caldwell, Director of Homeland and Justice Issues, Homeland Security and Justice Issues, Government Accountability Office. In this capacity, he provides direct support to congressional committees and to the individual Members of the House and Senate on Maritime Security and U.S. Coast Guard issues.

Ms. SANCHEZ. Welcome to all of you. And, without objection, your full testimonies will be inserted in the record. And I will now ask each witness to summarize his or her statement for 5 minutes, beginning with Mrs. Fanguy.

**STATEMENT OF MAURINE FANGUY, DIRECTOR,
TRANSPORTATION SECURITY ADMINISTRATION,
DEPARTMENT OF HOMELAND SECURITY**

Ms. FANGUY. Good afternoon, Madam Chairwoman, Ranking Member Souder, Chairman Thompson, and distinguished members of the subcommittee. My name is Maurine Fanguy, and I am the program director for the Transportation Worker Identification Credential program, also known as TWIC. Today I am here to show you the results of our efforts, the TWIC credential. In all of our previous meetings, we have talked to you about what we needed to do and what we are going to do. Now I would like to tell you what we have done.

Since I last testified before you in April, I am proud to say we have completed testing and have made significant advances in all aspects of the program. Most importantly, we began enrollments in Wilmington, Delaware on October 16. Enrollment is going well to date. We have enrolled more than 700 people and have more than 7,000 people pre-enrolled nationwide. Average enrollment time is under 15 minutes, and average wait time in Wilmington is about 6 minutes. These are real numbers that demonstrate real progress.

As we speak, our team is preparing to begin enrollments in Corpus Christi this Thursday, November 1. After we verify successful

operations in Corpus Christi on Thursday, we will issue the specific dates for the next 10 ports. Based on our progress to date, we are on track for mid November rollout in Baton Rouge, Beaumont, Honolulu, Oakland, and Tacoma. This group will be followed in late November by Chicago/Calumet, Houston, Port Arthur, Providence, and Savannah.

TWIC is one of the world's most advanced interoperable biometric credentialing programs and is powered by state-of-the-art technologies. As we continue to roll out across the Nation, TSA will vet as many workers in one day as we did in one year of prototype. That is over 5,000 workers a day. This program will impact hundreds of thousands of American workers who represent the backbone of global commerce. The start of enrollment represents a significant milestone in the program, and we have also taken other critical steps in our multi-layered approach to securing our Nation's ports.

First, we added 17 new TWIC enrollment sites based on stakeholder input. We understand the importance of making enrollment as convenient and accessible as possible. The additional sites bring the total number to fixed enrollment centers to 147 nationwide. We have also added mobile enrollment to take TWIC directly to the workers. Second, we reduce the price of a standard TWIC card to \$132.50. It is very important to us to limit the cost to workers as much as possible. Third, we publish technical specifications for TWIC biometric card readers. This allows industry to enhance access control technologies used at 3,200 facilities and on 10,000 vessels.

And, fourth, we held kickoff meetings with five card reader pilot participants. The Port Authorities of Long Beach, Los Angeles, New York and New Jersey, and Brownsville, as well as watermark cruises in Annapolis, were selected to represent a broad range of operating environments. We are continuing to meet with interested stakeholders to identify additional participants. We are pleased to have started in Wilmington, and look forward to the start of enrollment in Corpus Christi later this week. We will continue to work with our partners, the Coast Guard, maritime stakeholders, and this committee, to ensure the ongoing success of the TWIC program. We appreciate your support most recently in sending a staff delegation to Wilmington, and we look forward to hosting you at one of our enrollment centers soon.

Thank you for the opportunity to appear today, and I would be happy to answer any questions.

Ms. SANCHEZ. I thank the gentlelady.

[The statement of Ms. Fanguy follows:]

PREPARED STATEMENT OF MAURINE FANGUY

Good afternoon Chairwoman Sanchez, Ranking Member Souder, and distinguished members of the Sub-Committee. Thank you for this opportunity to share with you the significant progress we have made on the Transportation Worker Identification Credential (TWIC) program. I would like to acknowledge the leadership this sub-committee has provided in defining the vision for TWIC.

The TWIC program is moving towards its objectives while making sound decisions focused on enhancing port security and a reasoned, phased-in program implementation approach. I am happy to inform the Committee that TWIC enrollments began in Wilmington, Delaware, on Tuesday, October 16, 2007. After successful start-up in Wilmington, we will now proceed to Corpus Christi in early November. By mid-

November, enrollment will start in Baton Rouge, Beaumont, Honolulu, Oakland, and Tacoma. This group will be followed in late November by Chicago/Calumet, Houston, Port Arthur, Providence, and Savannah.

In addition to announcing the implementation of the program, we have made significant progress in other areas since our last appearance before this sub-committee:

- Implementation of the pre-enrollment capability;
- Completing test milestones on the enrollment system;
- Adding TWIC enrollment sites based on stakeholder input;
- Reducing the price of a TWIC card;
- Establishing reader technical specifications; and
- Identifying card reader pilot participants and holding kick-off meetings.

Completing Test Milestones on the Enrollment System

TWIC will impact hundreds of thousands of American workers essential to the smooth flow of global commerce. Once TWIC is up and running, TSA will vet as many workers in one day as we did during the entire year-long prototype. The importance and enormity of this task within the maritime environment, with a dynamic and mobile workforce, has demanded a methodical approach with rigorous testing.

TWIC will be one of the world's most advanced, interoperable biometric credentialing programs and is powered by state-of-the-art technologies. We have completed our "flight test" of the full TWIC system, which has five main components:

- **Pre-Enrollment Web Site:** allows workers to schedule appointments and provide information ahead of time to make enrollment easier.
- **Enrollment Center:** captures a worker's biometric and biographic information and submits the information for security processing.
- **TWIC Core System:** routes applicant information for processing, conducts data integrity checks, and manages the status of TWIC cards.
- **Screening Gateway:** aggregates security threat assessment data from the FBI, Citizenship and Immigration Services, and watchlists. It is important to note that the Screening Gateway is used across all of TSA's vetting programs.
- **Card Production:** electronically loads an applicant's information onto a TWIC smart card and then physically produces the card.

All five of these parts were first tested individually. Next, these pieces were integrated to ensure the functionality of the end-to-end process of conducting accurate and timely security threat assessments and producing high quality credentials. In addition, security and privacy requirements were validated throughout the process. After our contractor verified system readiness, TSA completed independent verification before beginning final test enrollments in the field using live vetting on government and trusted contractor personnel.

Today the switch has been turned on and the doors have opened with the commencement of enrollment in Wilmington, Delaware. After we verify successful enrollment operations in Wilmington, we will move forward to expand TWIC across the nation.

Adding TWIC Enrollment Sites

The TWIC final rule established a network of 130 enrollment sites located across the nation. Understanding the importance of making enrollment as convenient and accessible as possible, we have worked with maritime stakeholders, the Department, and our partners in the United States Coast Guard to add additional locations for TWIC enrollment centers. At this time, we will field 146 fixed enrollment centers. In addition, we have worked with our contractor to add a mobile enrollment capability to take TWIC to the workers.

Reducing the Price of a TWIC Card

TWIC is a fee-based program paid for by applicants. We fully realize that these costs are significant, and we are mindful of the need to identify areas for cost reduction. Recently, we announced that the fee for a standard TWIC will now be \$132.50, a decrease from the price anticipated in the Final Rule. Workers with current, comparable threat assessments including HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade (FAST) will receive a discounted fee of \$105.25. The cost of a lost, damaged or stolen credential is \$60.

Establishing Reader Technical Specifications

The TWIC technical architecture is compatible with the credentialing standards established in Federal Information Processing Standard (FIPS) 201-1. This alignment is critical to support card and reader interoperability within the maritime mode. In response to comments received on the initial TWIC Notice of Proposed Rulemaking (NPRM), TSA and the Coast Guard decided to remove the requirement

for biometric readers from the TWIC final rule to allow time to establish technology specifications to support maritime operations.

TSA and the Coast Guard sought the advice of the National Maritime Security Advisory Committee (NMSAC), which established a working group to collaboratively develop new technical specifications that complement FIPS 201-1 and add features that will support high-volume physical access in the harsh maritime environment. The working group included representatives from both the maritime and technology industries.

TSA recently published the TWIC reader hardware and card application working technical specification. The working specification establishes the requirements for biometric card readers for the pilot projects required by the SAFE Port Act. These readers will be tested during the pilot program. As the card and readers are envisioned to operate when TWIC is fully implemented, use of a PIN will not be necessary to release the biometric, unless the owner/operator chooses to use contact readers and the contact side of the credential.

Identifying Card Reader Pilot Participants and Holding Kick-Off Meetings

As required by the SAFE Port Act, we have initiated pilot programs with five partners across the country to test card readers. The pilots will test access control technologies in real world marine environments. Our current list of participants includes the Port Authorities of Los Angeles, Long Beach, Brownsville, and New York/New Jersey, in addition to Watermark Cruises in Annapolis, Maryland. As part of the outreach efforts for the TWIC program and the Department's Port Security Grant Program, we continue to seek additional participants. Our objective is to include pilot test participants that are representative of a variety of facility vessels which operate in a variety of geographic locations and environmental conditions. There appears to be sufficient interest from the maritime community to achieve this objective.

We are in the process of finalizing the test approach for the pilots. We are working with the Department of Homeland Security's Science and Technology component and the National Institute of Standards and Technology (NIST) to establish a test plan that will evaluate the card-reader interface under a variety of conditions and assess its impact on operations. Through the pilot tests, we will investigate the impacts of requiring biometric identity verification on business processes, technology, and operational impacts on facilities and vessels of various size, type, and location. As the program proceeds, the pilots will inform the TWIC reader rulemaking process and ultimately result in final regulations that require the deployment of transportation security card readers consistent with the findings of the pilot program.

Lessons Learned and Future Efforts

We are proud of the significant progress we have made in the past six months and are mindful of the challenges ahead. As we move forward in the TWIC program, we are committed to incorporating our lessons learned to drive sound management decisions geared at improving all aspects of the program, including:

- *Look for efficiencies by eliminating duplicative regulatory processes.* TSA and Coast Guard are developing procedures for the sharing of fingerprints, identity verification, criminal history, and photographs for TWIC which is expected to save not only money but time. In addition, merchant mariners will no longer be required to visit a Regional Exam Center to obtain and renew their credentials, resulting in substantial time and travel savings.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meeting with operators and associations, and contributions of advisory councils all added great value. We came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting our ports.
- *Address the impact on small businesses.* TSA and the Coast Guard worked closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas. We are also producing and distributing a Small Business Compliance Guide to assist small businesses in their implementation of the program.
- *When practical, preserve State regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, the TWIC regulations do not preempt States from requiring background checks and badging systems

for non-security purposes in addition to TWIC. States may need to set standards for important purposes other than terrorism threats, such as theft or organized crime.

- *Plan for privacy.* All data collected at an enrollment center will be completely deleted from the enrollment center work stations after transmission to TSA. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which is protected through role-based entry, encryption, and segmentation to prevent unauthorized use. No paper records with personal identification information are created in the enrollment process.

- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emerging needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin performance-based contract award is a culmination of our efforts to date. We will continue to look for and implement adaptive program planning, contractor oversight, and metrics to ensure the success of the program.

- *Plan to address what issues may arise during testing.* Evolving technology, such as card readers, create a changing environment and program control constraints. This is especially the case when the technology must be deployed to a vast multitude of entities with remote connectivity challenges (e.g., vessels) and varying degrees of access control system capabilities.

Conclusion

The steps we are taking will be an extremely important aspect to the security of our port facilities and vessels. TSA will continue to work with our partners, the U.S. Coast Guard and maritime stakeholders, to ensure that for the first time in history thousands of independent businesses will have one interoperable security network and workers will hold a common credential that can be used across that entire network.

I appreciate the keen interest that this Sub-Committee has in an effective implementation of TWIC, and I thank you for your support. Madame Chairwoman, this concludes my testimony, and I would be pleased to answer any questions that you may have.

Ms. SANCHEZ. And I now recognize Captain Sturm to summarize your statement in five minutes, please.

STATEMENT OF CAPTAIN FRANCIS STURM, DEPUTY DIRECTOR, CHIEF OF THE OFFICE OF PORT, VESSEL, AND FACILITY SECURITY, UNITED STATES COAST GUARD

Captain STURM. Good afternoon Chairwoman Sanchez, Ranking Member Souder, Chairman Thompson, distinguished members of the subcommittee. My name is Captain Frank Sturm, acting director of Prevention Policy for the U.S. Coast Guard. It is a pleasure to appear before you today to discuss the Coast Guard's efforts in implementing the SAFE Port Act requirements.

The primary objective of the SAFE Port Act is to improve maritime and cargo security through an enhanced layered defense. The Coast Guard has been intimately involved in achieving many of the Act's requirements. In the interest of time, I will address the key SAFE Port Act requirements which involve Coast Guard action.

The resumption of commerce and recovery of the Marine Transportation System, or MTS, following a significant disruption is a national issue of concern. The Maritime Transportation Security Act, or MTSA of 2002, required that the National Maritime Transportation Security Plan include a plan to restore cargo flow following a national transportation security incident. The Coast Guard held a national symposium in August of 2006 that resulted in specific recommendations on NTS recovery, and these are being jointly addressed within the Department of Homeland Security. These follow-up actions as required by section 101 of the Act in-

clude the development of salvage response plans within each area of Maritime Security Plan, or AMSP. The AMSP update is planned for completion by area maritime security committees during the summer of 2009 as part of the 5-year plan update cycle established by MTSA.

Section of 104 of the SAFE Port Act includes a number of statutory requirements governing the implementation of the Transportation Worker Identification Credential, or TWIC. The Coast Guard and TSA met the section's first deadline with the posting of the TWIC final rule on January 1, 2007. The TWIC rule, together with the Merchant Mariner Credential Rule, which was published on January 25, 2007, will allow mariners to apply for or renew Merchant Mariner credentials through the mail concurrently with the TWIC enrollment process, thereby eliminating travel to Coast Guard regional exam centers and removing duplicative background checks and other application redundancies.

The TWIC final rule also incorporates a background check process to enable newly hired workers to begin working while awaiting issuance of their TWIC. To enhance both the safety and security of vessels transiting our waters, the Act requires the establishment of a long-range automated vessel tracking system. This requirement demands a multi-faceted approach. Using the full range of classified and unclassified vessel tracking information, including some information purchased from some vendors where appropriate, the Coast Guard currently meets or exceeds the tracking requirements of the Act. The Long-Range Identification and Tracking Notice of Proposed Rulemaking was published in the Federal Register on October 3, 2007.

In accordance with section 113 the Coast Guard is supporting the Federal Emergency Management Agency, or FEMA, in implementing requirements relating to port security training. Collectively, progress has been made in establishing a program delineated in the Act. The Coast Guard and the Maritime Administration, or MARAD, have developed model courses for facility personnel to meet the requirements of 2002. These model courses establish a competency based standard and also cover the majority of the requirements of the SAFE Port Act.

In addition, FEMA has awarded a \$6.18 million cooperative grant to Florida State University to develop courses meeting requirements MTSA requirements and covering the eight port security related topics required under the SAFE Port Act.

Federal funds have also been awarded to assist ports with security enhancements. Over \$200 million in port security grant funding were available in fiscal year 2007. Initial reviews of the fiscal year 2007 grant applications were completed first by local captains of the port and then by a national review panel. Funds were awarded based on analysis of risk and the effectiveness of proposed investments, and results were announced on May 30, 2007. An additional \$110 million was provided by Congress in supplemental port security grant funding earlier this calendar year. Awards for this funding were announced in September of 2007.

Finally, in accordance with the Act, the Coast Guard has increased the pace of foreign port assessments and is on track to complete an initial assessment of all of our trading partners by

March of 2008. We intend to conduct assessments on a two-year cycle thereafter and continue capacity building efforts overseas.

In conclusion, the Coast Guard is committed to implementing all the various statutes within the SAFE Port Act. We continue to make headway on all fronts and look forward to future progress and partnerships with international, Federal, State, and local port organizations.

Thank you for the opportunity to testify today.

Ms. SANCHEZ. Thank you, Captain, for your testimony.

[The statement of Captain Sturm follows:]

PREPARED STATEMENT OF CAPTAIN FRANCIS J. STURM

Good afternoon Madame Chairwoman and distinguished members of the Subcommittee. I am Captain Francis J. Sturm, Acting Director for Prevention Policy under the Assistant Commandant for Marine Safety, Security and Stewardship at Coast Guard Headquarters. It is a pleasure to appear before you today to discuss the Coast Guard's efforts in implementing the Safety and Accountability for Every Port (SAFE Port) Act requirements one year after its implementation.

The objective of the SAFE Port Act is "to improve maritime and cargo security through enhanced layered defenses." The Coast Guard is cited as one of the primary organizations identified with specific responsibilities for implementing this overall objective. Several components within our organization have been involved in achieving the requirements since October 13, 2006 and I will address the SAFE Port Act requirements section-by-section.

We have had many successes to date in meeting the requirements of the SAFE Port Act, including requirements involving the inclusion of Salvage Response Plans in Area Maritime Transportation Security Plans (Section 101); Unannounced Inspections of Maritime Facilities (Section 103); the Port Security Training Program (Section 113); the Port Security Exercise Program (Section 114); and Foreign Port Assessments (Section 234).

We recognize, however, that there is still work to be done. There are some timeline requirements in the SAFE Port Act that we have not met, including those related to Notice of Arrival for Foreign Vessels on the Outer Continental Shelf (Section 109) and Enhanced Crewmember Identification (Section 110). We are committed to working closely and diligently with our DHS partners to meet these and other requirements of the SAFE Port Act.

Section 101 Area Maritime Transportation Security Plan to include salvage response plan

Development of Salvage Response Plans within each Area Maritime Security Plan (AMSP) has been integrated into the five-year plan update cycle established by the Maritime Transportation Security Act (MTSA) of 2002. The AMSP update will be performed by Federal Maritime Security Coordinators in consultation with their respective Area Maritime Security Committees and is planned for completion during early summer 2009.

A Salvage Response Plan will be a major element of the U.S. Marine Transportation System (MTS) recovery section of each AMSP and will provide the coordination and procedural foundation to support development of unified command incident action plans under the Incident Command System (ICS) construct when salvage response becomes necessary to facilitate resumption of trade. Authorities, capabilities, and other salvage issues are currently being coordinated with government and other partners. Consultation with national-level salvage industry representatives is continuing with the development of a Memorandum of Understanding (MOU) between the Coast Guard and the American Salvage Association. The MOU will establish a partnership with the goal of strengthening the communication and working relationship between the Coast Guard and the marine salvage and fire fighting industries to improve vessel and personnel safety; enhance national security preparedness and response; promote timely and professional salvage response to marine casualties; and enhance the protection of the environment along our nation's waterways.

Resumption of commerce and recovery of the marine transportation system (MTS) following a significant disruption is a significant national issue of concern. The Maritime Transportation Security Act (MTSA) 2002 required that the National Maritime Transportation Security Plan include a plan to restore cargo flow following a National Transportation Security Incident (NTSI). The Coast Guard held a National Recovery Symposium at the National Maritime Institute of Technology and Grad-

uate Studies on August 1st and 2nd, 2006. The symposium was attended by over 150 executive level participants from numerous branches of state and Federal government, as well as the private sector.

The Coast Guard is currently developing a concept of operations and specific planning requirements and organizational structures to ensure a focus on MTS recovery following a significant disruptive incident. MTS recovery guidance will be harmonized with, and support implementation of, the Strategy to Enhance International Supply Chain Security recently completed by the Department of Homeland Security with Coast Guard and interagency input. Implementation guidance will also harmonize with MTS recovery principles gleaned from Hurricane Katrina lessons-learned that have already been published in the U.S. Coast Guard Incident Management Handbook.

Review of maritime security developments since the implementation of MTSA, MTS recovery lessons from Hurricane Katrina, best Area Maritime Security practices from the field, and an update of MTSA implementation guidance are in progress. Review results to date have formed the basis for revising Navigation Vessel Inspection Circular 09-02 which is used to guide the five-year AMSP update.

Consistent with the overriding requirement to deter, and when necessary, mitigate the effects of Transportation Security Incidents (TSIs), the Coast Guard is working to make AMSP coordination and procedures "all-hazard and transportation disruption" compatible as much as practicable. This, in conjunction with oil and hazardous materials response coverage provided through Area Contingency Plans (ACP), application of Incident Command System (ICS) principles and structures per the National Incident Management System (NIMS), is intended to support an integrated and coherent preparedness approach across all transportation disruptions without requiring additional port-level plans.

Section 102 Requirements relating to maritime facility security plans

The Coast Guard recognizes that information on ownership of maritime facilities and the companies that operate them is vitally important to the management of the security posture and the clear delineation of security responsibilities within the port. Currently, in 33 CFR 104.415(b)(2), 105.415(b)(2), and 106.415(b)(2), the Coast Guard requires a security plan audit whenever the owner or operator of a vessel, facility or Outer Continental Shelf (OCS) facility changes. Should the audit reveal that an amendment to the security plan is necessary, the security officer of the vessel, facility or OCS facility will submit the amendment to the cognizant Captain of the Port or District Commander for approval. Consistent with the requirement in Section 102 of the SAFE Port Act, the DHS Appropriations Act of 2007 requires the Coast Guard to gather ownership information on vessel and facility security plans.

In order to meet the requirements in these statutes, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate these new ownership reporting requirements.

Implementation of the Transportation Worker Identification Credential (TWIC) regulations published in January 2007 will meet the requirement in Section 102 for a qualified individual having full authority to implement security actions for a facility to be a citizen of the United States, unless the Secretary waives the requirement after a determination based on a complete background check of the individual. These regulations, found in 33 CFR 105.205(a)(4), require facility security officers (the qualified individuals in the statute) to possess and maintain a TWIC. The security threat assessment conducted as part of the TWIC program involves a complete background check, including a criminal history records check, a legal status check, and an intelligence and terrorist watch list check, to satisfy the relevant mandate within this section. In addition, the Coast Guard is addressing the requirement for Facility Security Officers to be U.S. citizens in the regulatory project to update Subchapter H. A final fee was published on September 28th along with some modifications to the earlier rule.

Section 103 Unannounced inspections of maritime facilities

Currently, Coast Guard policy calls for an annual inspection of each facility, supplemented by periodic spot checks. The fiscal year 2007 Homeland Security Appropriations Act provided \$15M to, among other efforts, fund additional port security inspections. With this funding, the Coast Guard has created 39 new field billets to add to the current 350 facility inspectors. Thirty-seven of these new billets were filled during the 2007 transfer season, and the remaining two are in the process of being filled. The Coast Guard conducted more than 7,500 annual inspections and spot checks of 3,200 facilities in calendar year 2006. We have also applied additional reserve billets this year to increase facility visits and ensure each facility is inspected not less than two times this year. At least one of those inspections will be unannounced.

Section 104 Transportation security card

Section 104 of the SAFE Port Act includes a number of statutory requirements relating to the implementation of the TWIC program. The effort to promulgate TWIC requirements through the rulemaking process met its SAFE Port Act deadline of January 1, 2007 with the posting of the TWIC Final Rule. This rule, together with the Merchant Mariner Credential Supplemental Notice of Proposed Rulemaking published on January 25, 2007, will allow mariners to apply for or renew merchant mariner credentials through the mail concurrently with the TWIC enrollment process, eliminating travel to Coast Guard Regional Exam Centers and removing duplicative background checks and other application redundancies which exist under each program. Also, the TWIC final rule incorporates a background check process to enable newly hired workers to begin working while awaiting issuance of their TWIC, in accordance with the Act.

The Coast Guard continues to support the Transportation Security Administration's (TSA's) efforts to implement the TWIC program by providing field and industry guidance to assist with compliance and enforcement activities. In addition, the Coast Guard is working closely with DHS and TSA on the pilot program to test the implementation of card readers to provide critical information and lessons to inform a second rulemaking to address TWIC readers. As part of our support for this effort, the Coast Guard, jointly with TSA, charged the National Maritime Security Advisory Committee (NMSAC) to form a working group of maritime industry and biometric technology representatives to propose specifications for TWIC cards and card readers using a contactless (or proximity) interface. The NMSAC presented recommended specifications on February 28, 2007. A notice of availability of the specifications was published in the Federal Register for public comment on March 16, 2007 and the notice of availability of the final contactless specification was published in the Federal Register on September 20, 2007.

Work continues on several aspects of the TWIC Program. The Coast Guard intends to purchase handheld card readers in fiscal year 2008 for use during vessel and facility inspections and spot checks. After the compliance date passes in a given port, the Coast Guard will use the card readers to randomly check the validity of an individual's TWIC. Also, the provision for newly hired employees to work while they await issuance of a TWIC is in development and on track. The Coast Guard has received stakeholder comments on policy and included them in the form of a Navigation and Vessel Inspection Circular (NVIC) which provides guidance and instruction on how to implement TWIC regulatory requirements for access control on facilities and vessels. This NVIC was published in July 2007.

Section 107 Long-range vessel tracking

The Coast Guard currently meets the intent and requirements of the Act, using the full range of classified and unclassified vessel tracking information available. However, it takes up to two years to develop and finalize a regulation. While the Long Range Identification and Tracking (LRIT) NPRM did not meet the April 1, 2007 deadline, it was published in the Federal Register on October 3, 2007. The Act requires the DHS Secretary to establish a long range automated vessel tracking system that meets the following:

- Tracking: Provided for all vessels in U.S. waters equipped with Global Maritime Distress and Safety System (GMDSS) or equivalent satellite technology; and
- International: Consistent with international treaties, conventions and agreements.

Tracking:

The SAFE Port Act requirement demands a multi-faceted approach. Using the full range of classified and unclassified vessel tracking info available, including some information purchased from vendors where appropriate, the Coast Guard currently meets and exceeds the tracking requirement of the Act. Currently, sufficient tracking information exists; however more work is needed in processing, display, and training in the use of this information.

International:

Our work to establish a system through the International Maritime Organization (IMO) will provide an unclassified global tracking capability in 2008 as a part of an existing IMO convention and give the United States a system that is compatible and interoperable with the global maritime community. The Coast Guard has been working with the IMO since shortly after 9/11 to implement a global tracking system for the types of vessels described in the Act. Following considerable diplomatic efforts, the international agreement to implement such a system was reached last year, and the global tracking system will be in effect at the end of 2008. In the long run, this approach is more advantageous to the United States because it applies glob-

ally to all the world's ships of the kind described by the Act instead of just those in U.S. waters or vessels intending to make ports call in the United States. Under this system, the U.S. will have access to information for U.S. Flag vessels regardless of their current location, and vessels bound for U.S. ports when they declare intent to arrive. Information on all other vessels will be available whenever a ship is within 1,000 nautical miles of the U.S. coast. The Coast Guard is examining funding strategies for this important international system.

To complement the above activities, the Coast Guard also initiated a rulemaking to implement in Title 33 of the Code of Federal Regulations rules that require ships to report identifying and position data electronically. These rules provide guidance to U.S. and foreign ships on how to comply with this new reporting requirement, as well as an additional enforcement mechanism for ships that fail to comply.

Section 108 Establishment of Interagency Operational Centers for Port Security

Section 108 requires a budget and cost-sharing analysis for implementing interagency operations centers. The report required by this Section was submitted in July. It identified the estimated total acquisition cost of upgrading the 24 Coast Guard Sector Command Centers (SCCs), which encompass the Nation's high priority ports, as approximately \$260 million. The major cost elements of this five-year project plan include an information management software suite, a sensor package and facility recapitalization.

The establishment of interagency operations centers is currently not funded. In cooperation with the Department of Justice (DOJ), the U.S. Navy, and the DHS Office of Science and Technology, five prototype centers have been established to date. These centers are each configured differently as test beds for concepts, tactics, procedures and equipment. Cost sharing arrangements exist among the various participants.

Designator	Location	Cost-Sharing Agencies
Seahawk Joint Task Force	Charleston, SC	Dept. of Justice/U. S. Coast Guard.
SCC*-Joint	Hampton Roads, VA	U. S. Coast Guard/U.S. Navy.
SCC-Joint	San Diego, CA	U.S. Coast Guard/U.S. Navy.
SCC-Joint	Jacksonville, FL	U.S. Coast Guard/U.S. Navy.
SCC-Joint	Seattle, WA	U.S. Coast Guard/U.S. Navy.

*Sector Command Center

Additionally, seven ports have been identified for short and medium term pilot projects to evaluate joint operations design models between the Coast Guard and Customs and Border Protection (CBP). These pilots will include examination of methods for implementation of a virtual command center construct using various collaboration tools for daily coordination and vessel inspection planning.

Command 21, when funded, will field the capabilities necessary to create interagency operations centers as required by Section 108. This establishment of proposed interagency operational centers for port security is a major system acquisition tailored to each port and designed to close gaps in port and coastal maritime security.

Command 21 will:

- Improve maritime port and coastal security systems to complement Secure Border Initiative (SBI) Net;
- Improve unity of effort in a multi-agency operations center environment;
- Accelerate deployment of a net-centric tactical system that implements DHS enterprise standards for the sharing of situation data and services across multiple DHS interagency domains and Coast Guard systems; and
- Counter the small vessel threat in port and coastal areas.

The Coast Guard's experience with interagency operations centers demonstrates that many tangible benefits to improve maritime safety, security, and stewardship can be achieved. Some of these include:

- Cooperative targeting and coordination of intelligence facilitates information sharing;
- Daily field-level coordination breaks down barriers between agencies;
- Collective use of tactical sensors (radars/cameras) saves time, money and effort;

- Cooperative planning improves readiness and efficiency; and
- Sharing of law enforcement information helps reduce criminal activity in the port and cut off potential funding to terrorist groups.

Command 21 will close a critical gap between current capabilities and the desired interagency end state. Future interagency operations will be greatly improved as all partners will be able to:

- **See** maritime activities using port surveillance sensors;
- **Understand** the scene by automatically bringing tactical and intelligence information together; and
- **Share** this tactical data with each other as they work side by side in improved facilities.

To close the gap between the current Sector Command Center (SCC) capabilities and the future state desired by the Act, the Coast Guard must field a sensor network and an information system allowing the centers to monitor maritime activities in critical areas. That system must link vital data on vessel history, crew, and cargo to the activities observed. The current SCC facilities must also be sufficiently expanded to host port partners in an interagency operations environment, as directed by the SAFE Port Act and the Maritime Transportation Safety Act.

Command 21 will publish tactical data in an open standard that allows other systems across multiple DHS domains to subscribe to the information and use according to the individual needs of each agency. It provides the maritime component of the Department of Homeland Security's Secure Border Initiative (SBI). Good government demands that both programs move forward in parallel to increase deterrence capabilities. Moving ahead on both fronts will provide collaborative opportunities to leverage critical resources to broaden the impact of both programs toward securing our borders.

Section 109 Notice of arrival for foreign vessels on the Outer Continental Shelf

The regulations for Notice of Arrival for foreign vessels on the Outer Continental Shelf (OCS) have been developed and incorporated into an existing Coast Guard rulemaking project related to OCS activities. This rulemaking, the updating of 33 CFR Subchapter N, "Outer Continental Shelf Activities," already includes Notice of Arrival requirements for foreign vessels operating on the OCS. The Coast Guard has completed evaluation of the proposed regulations and public comments, and an interim rule will be issued to implement the provisions of Section 109 as expeditiously as possible. The earliest anticipated action would be an Interim Rule by March 2008. If an NPRM is required, anticipated completion time would be at least two years.

Section 110 Enhanced crewmember identification

Historically, the Coast Guard advanced the effort to negotiate the international seafarer's identification initiative at the International Labor Organization (ILO), resulting in the ILO-185 Seafarer's Identification Document (SID). However, a requirement within ILO 185 prohibiting implementing nations from requiring a visa for seafarers holding a SID to be eligible for shore leave has prevented the U.S. from ratifying ILO 185.

In accordance with the Act, the Coast Guard has prepared a draft NPRM defining the identification documents necessary for all foreign mariners calling on U.S. ports. The proposed identification requirements would also apply to US mariners arriving at U.S. ports from a foreign port of place of departure.

Section 111 Risk assessment tool

The Maritime Security Risk Analysis Model (MSRAM) is being used by Captains of the Ports/Federal Maritime Security Coordinators (FMSCs) and Area Maritime Security Committees (AMSC) to analyze and prioritize scenario-based risks within their areas of responsibility, and to measure risk reduction potential in the evaluation of port security grant program proposals. FMSC and AMSCs are required to validate the MSRAM data on an annual basis. This was last completed in the summer of 2007 using MSRAM version 2.

Section 112 Port security grants

The Coast Guard worked with the DHS Office of Grants and Training, who has fiduciary responsibility for the Port Security Grant Program, to complete the report to Congress required by this Section. The report was submitted to Congress on April 27, 2007.

The Port Security Grant Program (PSGP) provides grant funding to port areas for the protection of critical port infrastructure from terrorism. fiscal year 2007 PSGP funds are primarily intended to assist ports in enhancing risk management capabilities; domain awareness; capabilities to prevent, detect, respond to and recover from

attacks involving improvised explosive devices (IEDs) and other non-conventional weapons; as well as training and exercises.

\$201,670,000 was available for Port Security Grants in fiscal year 2007. These funds were divided amongst four tiers of ports. Within Tier I, eight of the highest risk port regions were allocated a fixed amount of funding based on risk. In many cases, multiple port areas were grouped together to reflect geographic proximity, shared risk, and a common waterway. Port areas submitting applications within Tier II and III were eligible to compete for the fiscal year 2007 PSGP but were not guaranteed funding. Section 112 of the SAFE Port Act also required that any entity addressed in an Area Maritime Security Plan also be eligible to apply. Tier IV was established for those new entities not within the port areas in Tiers I–III. This added approximately 259 ports to the 102 highest risk ports for a total of 361 that were eligible to compete, but were not guaranteed funding.

Funds were awarded based on analysis of risk and effectiveness of proposed investments by the applicants. Risk to port Infrastructure Protection Program Detail areas was assessed using a methodology consisting of threat, vulnerability, and consequence factors. The majority of port security grant funds—\$120.6 million—was allocated to eight Tier I ports or port areas that we consider to be the highest risk.

Grant applicants had 60 days from January 6, 2007 to complete this process for the remaining \$81M. Applications were required to be submitted electronically via the grants.gov web site no later than March 6, 2007. The initial reviews were completed by the local Captain of the Port. These results were forwarded to a national review panel comprised of representatives from the Coast Guard, the Transportation Security Administration (TSA), DHS Infrastructure Protection (IP), Grants and Training (G&T), the Domestic Nuclear Detection Office (DNDO), and the Maritime Administration (MARAD) that convened on April 9, 2007. The results were announced on May 30, 2007.

The \$110 million was provided by Congress in supplemental Port Security Grant Funding (P.L. 110–28, the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007). Using the same risk-based analysis utilized during the initial fiscal year 2007 Port Security Grants, funds were allocated to Tier I and II ports to develop a Port-Wide Risk Management/Mitigation and Business Continuity/Resumption of Trade Plan which will identify a prioritized listing of items to be addressed within future grant applications. Tier III ports that previously submitted projects under the initial fiscal year 2007 PSG Program which were validated but unfunded, are to be funded with the Supplemental Grant. Tier IV ports also applied for TWIC and Training under the Supplemental Grant funding. The application period has closed. Both field and national review of the Supplemental applications have been completed, with announcement of all awards completed in September 2007.

Section 113 Port Security Training Program

The Coast Guard is supporting the FEMA National Preparedness Directorate's National Integration Center through Training and Exercises Integration (formerly known as the DHS Preparedness Directorate, Office of Grants and Training Division). Collectively, we are making progress in establishing the program delineated in the Act. There are a number of existing initiatives and new initiatives that will address the requirements in this section.

In response to Congressional mandate, the Coast Guard and MARAD developed model courses for the training of facility and other personnel to meet the requirements of the Maritime Transportation Security Act of 2002. These model courses establish a competence based standard and contain most of the requirements under this Section of the Act. The model courses were developed in support of the facility security plan requirements, and apply to all personnel working in a port facility or required to enter a port facility in response to an emergency. These model courses are available via website to Federal, state and local personnel from the public and private sector and they are undergoing a review to include lessons learned and the additional topics required under the Act. To ensure quality training, Coast Guard and MARAD developed and implemented a voluntary course acceptance and certification process using the model courses as the guidelines for acceptance. The Coast Guard is currently revising the regulations for security training for facility personnel to ensure all training is measured against a standard of competence, including the topics required under the SAFE Port Act.

The FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has awarded a \$6.18 million Cooperative Grant to the Florida State University to develop courses meeting the Maritime Transportation Security Act of 2002 requirements (model courses), and covering the eight port security-related topics required under the Act. MARAD and the Coast

Guard are actively assisting DHS to ensure this training will be consistent with existing standards and will provide the maximum possible return on investment. It is envisioned that these courses will be available for in-classroom and on-line training; and will be available both to Federal, state and local personnel as well as members of the private sector who work in the port security realm.

In addition, the FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has made available other training courses that address individual port security topics required under the Act. These courses are provided to State and local emergency responders and other identified audiences by Training and Exercises Integration, and are coordinated by each State's governor-designated Training Point of Contact.

Section 114 Port Security Exercise Program

Current port security exercise programs conduct live, risk-based exercises that are realistic and evaluate total capability by focusing on the port community, in order to evaluate the entire capability. These exercises involve State and local governments, as well as facilities and vessels, to ensure that consistent methodology is applied and that all requirements are met as a result. Although current programs do not mandate facility participation in these annual exercises, participation has been strong and continues to increase. Facilities, as well as vessels, are encouraged to observe and/or participate in these port security exercises. When they choose to participate, they are offered the opportunity to put forth exercise objectives tailored to meet their specific needs.

Since January 2005, the Coast Guard has assisted TSA in implementing their Port Security Training and Exercise Program (PortSTEP). Similarly, since October 2005, the Coast Guard has sponsored its own Area Maritime Security Training and Exercise Program (AMStep) that exercises the port stakeholder's ability to implement the provisions of the Area Maritime Security Plan. The Coast Guard and TSA have synchronized AMStep and PortSTEP to maximize coverage across the U.S. and minimize duplication of effort. In fiscal year 2007, these two programs collectively sponsored 41 port security exercises. Exercise types have included basic and advanced table-top, discussion-based exercises to full-scale, operations-based exercises. The type of exercise and scenario selected are collectively decided upon by Area Maritime Security Committee (AMSC) members, through application of their most current risk-based port assessment and assessment of preparedness needs. The results of both these exercise programs and all lessons learned, best practices, and corrective actions are documented in a semi-annual report to Congress.

The "Training" aspect of current port security exercise programs focuses on the National Incident Management System (NIMS) Incident Command System (ICS). Training, such as I-200 (Basic), I-300 (Intermediate) and I-320 (Team training), is offered to the entire port community prior to each annual exercise. Security-specific training is provided from within the port community.

Initial performance measures for port security exercises were established under Coast Guard NVIC 09-02, Change 2. These measures, outlined as objectives, are currently being revised by the Coast Guard to align with MTSA requirements to test the AMSPs and with the Homeland Security Exercise and Evaluation Program. All Lessons Learned, Best Practices, and Remedial Action Items are captured in the Coast Guard's Contingency Preparedness System (CPS), which can be accessed by the entire Coast Guard. Additionally, through the use of Homeport, the Coast Guard's communications and collaborations Information Technology application, Lessons Learned and Best Practices, can be made available to the entire port community (Federal, state, local, tribal and industry).

Although AMStep is currently being carried out under contract support, the Coast Guard has begun the hiring of personnel to staff National-level and Regional-level exercise support teams. These teams will assist Coast Guard Sector Commands (port-level) and Districts with the following contingency exercise programs: port security, oil/hazardous substance response, natural disaster, mass rescue, alien migration interdiction, civil disturbance, counterterrorism, military outload, combatant commander support, and physical security/force protection. This is an "All Threats / All Hazards" approach.

Section 115 Facility exercise requirements

Current regulations in 33 CFR 105.220(c) require facilities to conduct an annual exercise. These exercises may include either live, tabletop, or participation in a non-site-specific exercise. In order to meet the requirement in Section 115, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate definition of "high risk facility" and the requirement for high risk facilities to conduct bi-annual full-scale exercises. The NPRM for this rule-making is scheduled to be published in the spring of 2008.

Section 128 Center of Excellence for Maritime, Island and Extreme/Remote Environment Security

The Coast Guard is assisting the DHS Science and Technology (S&T) Directorate to meet the requirements of Section 108. The Broad Area Announcement (BAA) for a Center of Excellence (COE) for Maritime, Island and Extreme/Remote Environment Security was announced at the beginning of February 2007. This BAA incorporated Maritime Domain Awareness (MDA) study as a central component of a broader system of research into maritime security. This solicitation is still open, and there has been good response from the academic community. DHS S&T expects to award the COE by the end of 2007. The Coast Guard looks forward to this important new research component that will support DHS.

Section 201 Strategic plan to enhance the security of the international supply chain

The Coast Guard assisted the Department of Homeland Security's authoring team in drafting the required Strategy to Enhance International Supply Chain Security, providing lead authors for sections on response and recovery. Looking forward, the Coast Guard is working to structure the first required five-year update to Area Maritime Security Plans (AMSP) to position them to support field-level implementation of the strategy as it pertains to Transportation Security Incidents (TSI). A planning objective is to make these community-based coordination arrangements and procedures compatible for application during other forms of transportation disruption, insofar as practicable. We assigned the same Coast Guard subject matter experts to support each initiative, thereby facilitating content alignment for this purpose.

Section 233 International cooperation and coordination

The Coast Guard has been working with a variety of international organizations including the Asia Pacific Economic Cooperation (APEC) Forum, the Group of Eight (G8), and the Organization of American States (OAS) to conduct capacity building activities to improve the port security regimes of developing countries. Coast Guard representatives serve on maritime security expert groups of these organizations and have been intimately involved in identifying and executing projects.

Of particular note is our work with the OAS, an organization that is specifically mentioned in the SAFE Port Act for close coordination. Through the Inter-American Committee on Counter-Terrorism (an OAS body), and in conjunction with Canada, the Coast Guard is developing a series of exercises and best practice conferences. The first port security exercise was completed in Argentina in September 2007.

"The North Pacific Coast Guard Forum has had some notable successes in the area of joint operations recently, and the North Atlantic Coast Guard Forum will hold its first meeting late in October in Sweden."

Section 234 Foreign port assessments

The Coast Guard has increased the pace of assessments and is on track to complete an initial assessment of all of our trading partners by March 2008. The Coast Guard intends to conduct assessments on a two year cycle thereafter.

This two year cycle is consistent with the guidance contained in the fiscal year 2007 DHS Appropriations Act, which called on the Coast Guard to double the rate of assessments (basically from three per month to six per month). This reassessment cycle actually exceeds the requirement of the SAFE Port Act which call for reassessments to be conducted on a three year cycle. Additional resources (approx. \$6.7M and 32 FTE) provided in the fiscal year 2007 DHS Appropriations Act support this increase in activity.

Section 303 Research, development, test, and evaluation efforts in furtherance of maritime and cargo security

DHS and the Coast Guard have current and planned efforts to support the furtherance of maritime and cargo security. The Coast Guard RDT&E efforts for fiscal year 2007 include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications	<ol style="list-style-type: none"> 1. Maritime Biometrics, ID at Sea 2. Boarding Team Connectivity 3. Next Generation Underway Connectivity 4. Boarding Officer Tools and Equipment Support
Compel Compliance	<ol style="list-style-type: none"> 1. Anti-Personnel 2. Stopping Mid-Sized Vessels

Mission Areas	Programs/Projects
Platforms and Sensors	1. Acoustic Buoy 2. Multi-Sensor Performance Prediction 3. Global Observer 4. Small UAS Evaluations
Sector and Port Security Operations	1. Maritime Domain Awareness Community of Interest 2. National Automatic Identification System
Miscellaneous	1. Net-Centricity 2. Weapons of Mass D

Mission Areas	Programs/Projects
Boarding Team Support and Communications	1. Boarding Team Communications
Sensor, Data Fusion, & Decision Aids (Maritime)	1. Visualization Tools 2. Hawkeye Watch keeper Prototype 3. Offshore Buoys for Vessel Detection 4. Emergence Response Blue Force Tracking 5. Swimmer/Diver Detection 6. Global Observer

DHS S&T fiscal year 2008 funding has yet to be defined. The Coast Guard is planning a comparable dollar figure to support the furtherance of maritime and cargo security in fiscal year 2008. Through the DHS S&T established Capstone Integrated Product Teams (IPT), fiscal year 2009–2013 funding has been identified for the furtherance of maritime and cargo security through the Maritime Security Capstone IPT and the Cargo Capstone IPT.

Conclusion

The Coast Guard is committed to implementing the Security and Accountability for Every Port Act. We continue to make headway on all fronts and look forward to future progress and partnerships with international, Federal, state, and local port organizations. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Ms. SANCHEZ. And I now recognize Mr. Winkowski to summarize his statement for 5 minutes.

STATEMENT OF THOMAS WINKOWSKI, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION

Mr. WINKOWSKI. Good afternoon, Chairwoman Sanchez, Ranking Member Souder, and Chairman Thompson and distinguished members of the committee. Thank you for this opportunity to discuss with you today the status of U.S. Customs and Border Protection's efforts since the passage of the SAFE Port Act one year ago.

I would first like to thank Congress and in particular this committee for your continued interest in the important subject of maritime and supply chain security. As you know, CBP has developed and implemented unprecedented initiative to achieve our twin goals of both strengthening the security of cargo entering our borders and facilitating the flow of legitimate trade and travel. CBP uses a multi-layer approach to ensure the integrity of the supply chain from the point of stopping through vessel arrival at U.S. ports of entry. This multi-layered approach includes a use of trained CBP officers, technology automation, electronic information, and partnerships with the trade and foreign governments.

I would like to take a moment to highlight some of the important accomplishments that demonstrate how far we have come since September 11, and provide insight on some of the efforts CBP has made over the last 12 months to meet the requirements of the SAFE Port Act.

CBP, through the Container Security Initiative, and in coordination with the Department of Energy's megaport program, has partnered with other countries to deploy personnel and technology in an effort to prevent terrorists and terrorist weapons from entering the United States. Today, CSI is now operational in 58 ports covering 86 percent of the maritime containerized cargo shipped to the United States. At these 58 locations worldwide, CBP officers and ICE agents working alongside their host government counterparts identify the highest risk cargo and perform examinations before the cargo is laden on board a vessel destined for the United States, and CBP continues to enhance and improve upon this program for the Secure Freight Initiative.

I am pleased to announce that on October 13, the first phase of SFI became fully operational at three ports, thus meeting the requirements of the SAFE Port Act. Through a successful partnership of DHS and Departments of Energy and State, containerized shipments from Pakistan, Honduras, and United Kingdom, South Hampton, now undergo 100 percent scanning before the containers are loaded on their vessel destined for the United States. Surpassing the SAFE Port Act requirements, DHS is also partnering with four of the world's largest container ports to further explore the concept of 100 percent scanning in the real world environment, Singapore, Busan, Oman, and Hong Kong.

The size and complexity of these larger ports require initial limited deployment and will enhance our understanding of the challenges of 100 percent scanning in high volume and trans-shipment ports. DHS will submit a report to Congress in April 2008 detailing the progress made under SFI. The data experience and lessons learned from the initial phase of SFI will provide necessary insight into the practicality and benefits of 100 percent scanning, and will certainly guide any decisions regarding the potential expansion of SFI.

One of the key components of CBP's layered defense is the advanced electronic cargo information required of all modes of transportation by the Trade Act of 2002, the SAFE Port Act mandated provisions of additional data elements for four improved high-risk targeting and the overall enhancements targeting system.

Working with the advisory committee on commercial operations, CBP has proposed a new security filing better known as 10-plus-2 in an effort to obtain additional advanced cargo information and enhance our ability risk-based targeting. Under this initiative, the importer's designated agent will file 10 new unique data elements not currently provided to CBP, while carriers will provide stow-plan data and container status messages.

C-TPAT. Another important layer of our strategy is a C-TPAT program. Under C-TPAT, CBP works in partnership with the trade community to better secure goods moving through the international supply chain. As of October 26, there were 7,800 companies certified in the C6,100 validations in 85 countries today, with another

800 validations in progress which will be complete by year's end. CBP's goal is to meet the SAFE Ports Act requirement and to validate all members within one year of certification, and revalidate all validated members not less than once every 4 years.

Working with COAC, CBP has also developed and implemented a pilot program using third parties to validate supply chains where CBP currently lacks full access.

In May 2007, CBP selected 11 firms to act as validators in China. Interest in the pilot program has thus at minimum over 300 C-TPAT importers were invited to participate in this voluntary program in June, and to date less than a dozen importers have opted to do so. Upon conclusion of the pilot in June 2008, we will provide a full report on the effectiveness of using third-party firms to perform C-TPAT validations.

With that, I conclude my comments and look forward to your questions.

Ms. SANCHEZ. Thank you.

[The statement of Mr. Winkowski follows:]

PREPARED STATEMENT OF THOMAS S. WINKOWSKI

Introduction

U.S. Customs and Border Protection (CBP) appreciates this opportunity to discuss with you today the Security and Accountability For Every Port Act (SAFE Port Act) and the efforts of CBP nearly one year after its passage.

It is noteworthy that CBP worked quite closely with the House and Senate in the development of the SAFE Port Act and applaud the high level of Congressional interest in securing United States ports and the global supply chain. Much of what is in the SAFE Port Act codified initiatives that the U.S. Customs Service, now CBP, undertook immediately after 9/11 and has been implementing successfully ever since.

Below are updates on the primary areas of activity being undertaken by CBP to fully implement the Act.

Container Security Initiative (CSI)

To meet the priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries through the Container Security Initiative (CSI) to deploy multi-disciplined teams to selected foreign seaports to identify cargo containers that pose a potential risk for terrorism and inspect those containers at the foreign ports before they are shipped to the United States. CSI is an example where the SAFE Port Act codified existing DHS programs, and CBP is in compliance with the Act's mandates.

Almost 32,000 seagoing containers arrive and are off loaded at United States seaports each day. In fiscal year 2006, that equated to 11.6 million cargo containers annually. Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist exploitation. CSI's effectiveness and successes can be measured by several factors. At its core is the cooperation and information sharing between the CBP officers in the foreign seaports and the host government personnel. Additionally, CSI has been instrumental in enhancing port security. Through CSI, many foreign ports that previously did not utilize or possess non-intrusive inspection (NII) equipment now have either purchased their own or have access to NII equipment. Additionally, CSI has partnered with Department of Energy's Megaports Initiative at several CSI ports to further enhance the host nation's capability to screen cargo for nuclear and other radioactive materials that could be used by terrorists against the United States or a host country. This fiscal year CSI expanded to 8 additional ports, and reached a milestone of 58 ports worldwide covering 85% of the container traffic destined to the United States. This is significant progress.

Secure Freight Initiative (SFI) and 100% Scanning

Building upon the success of the Container Security Initiative (CSI), on December 6, 2006, the Secretary of Homeland Security, in cooperation with the Department of Energy (DOE), Department of State (DOS) and with the maritime industry and foreign government partners, announced Phase One of the Secure Freight Initiative (SFI). SFI is an unprecedented effort to build upon existing port security measures

by enhancing the United States government's ability to scan containers for nuclear and radiological materials in seaports worldwide and to better assess the risk of inbound containers.

I am pleased to announce that the first phase of SFI became fully operational on October 12, 2007 at three ports meeting the requirements of the SAFE Port Act. Southampton, United Kingdom, Puerto Cortes, Honduras and Port Qasim, Pakistan are now scanning 100% of containers destined for the United States.

The initial phase of the SFI involves the deployment of a combination of existing technology and nuclear detection devices to three ports as per the requirements of the SAFE Port Act. This will provide a more complete analysis for SFI by including different operational and geographic settings at each port and will provide exposure of different models for future 100 percent scanning. In addition to the first three ports, SFI Phase I will also include four additional ports that will conduct 100% scanning in a more limited capacity. Those ports are Port Salalah, Oman, Brani Terminal at Port of Singapore, Gamman Terminal at Port Busan, Korea, and the Modern Terminal in Hong Kong.

By conducting the pilot at these four additional ports, this new, integrated technology can meld smoothly into the logistics, operations, and risk management process while complementing the flow of commerce at high-volume and transshipment ports. Additionally, this first phase of SFI will provide the partnering governments with a greater window into potentially dangerous shipments moving through their seaports. Secure Freight will provide carriers of maritime containerized cargo with greater confidence in the security of the shipment they are transporting, and it will increase the likelihood for shippers and terminal operators that the flow of commerce will be both uninterrupted and secure. SFI will use the latest scanning technology, however data analysis, using the Automated Targeting System, will continue to be our primarily method in screening containers.

The lessons learned and experience gained from Phase One represent critical steps in the process of determining whether the concept of 100% overseas scanning is technologically and economically feasible and the degree to which it increases the security of the international supply chain.

DHS will submit reports to Congress in February and April 2008 detailing the progress made under SFI. These reports will also outline the successes and challenges associated with the implementation of 100% scanning in foreign locations, including issues related to the availability, capabilities and efficiency of technology and equipment; the process of negotiations/discussions with host nation counterparts as well as foreign input and feedback; the impact on the movement of cargo through ports and across the global supply chain; the staffing and human capital requirements that will be necessary both abroad and domestically and numerous additional considerations.

Domestic Radiation Detection and Imaging

The SAFE Port Act requires that a deployment strategy plan be developed for the placement of radiation portal monitors (RPMs) throughout the nation's ports of entry. That plan has been submitted to Congress by the Department.

CBP began deploying RPMs in October 2002, with the first deployment at the Ambassador Bridge in Detroit. Since that time, CBP and the Domestic Nuclear Detection Office (DNDO) have deployed over 1,000 RPMs at mail facilities, seaports, and land border crossings and will deploy the first RPM in the air cargo environment by the end of calendar year 2007. Specifically, the SAFE Port Act mandates that all containers entering through the top 22 seaports be scanned for radiation. Currently, the Department has deployed radiation detection equipment to each of these 22 ports. Due to unique operational considerations at some of these ports, not every terminal within a port is currently equipped with such equipment. However, to satisfy the requirements of the SAFE Port Act and to further enhance port security, CBP and DNDO continue to work with these considerations, and by the end of this calendar year will scan approximately 98% of all containerized cargo at these 22 seaports.

With the additional deployment of radiation scanning equipment, CBP currently scans 91% of the cargo and 81% of the passenger vehicles arriving from Canada; 97% of the cargo and 92% of the passenger vehicles arriving from Mexico, as well as 93% of arriving sea-borne cargo containers. To put this in perspective, just 18 months ago CBP was scanning 37% of arriving sea containers.

Additionally, CBP has deployed over 1,000 Radiation Isotope Identifier Devices (RIID) and over 16,000 Personal Radiation Detectors (PRD). These devices allow CBP to inspect 100% of all identified high-risk cargo.

Since CBP began scanning conveyances for radiation, over 195 million conveyances have been scanned, and over 1.1 million alarms have been resolved. This is

a tremendous workload, and the SAFE Port Act authorized 200 new CBP Officers in each of the next five years to help accomplish this mission. Furthermore, the Department is currently testing the next generation of radiation detection equipment known as Advanced Spectroscopic Portals at eight locations nationwide—at Piers A and J in Long Beach, at the APM and PNCT Terminals in Newark, at the Colombia and World Trade bridges in Laredo, at the Blue Water Bridge in Port Huron, and at the Fort Street crossing in Detroit. Future deployments of ASPs, pending Secretarial certification, will allow CBP to quickly differentiate between benign materials such as kitty litter or granite, while determining which shipments pose a true risk. This perfectly supports CBP's twin goals of increasing security while facilitating the flow of legitimate trade and people.

In addition to the deployment of radiation detection equipment, CBP continues to deploy large scale imaging systems and has deployed 195 large-scale gamma ray or x-ray imaging systems nationwide. NII technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of the container and the manifest. In fact, well over 5.5 million scans using NII systems were conducted in FY 07.

Automated Targeting System (ATS)

CBP requires advanced electronic cargo information as mandated in the Trade Act of 2002 (including the 24-hour rule for maritime cargo). Advanced cargo information on all inbound shipments for all modes of transportation is effectively evaluated using the Automated Targeting System (ATS) before arrival in the United States. The SAFE Port Act requires CBP to seek additional data elements for ATS as well as to evaluate the entire system. CBP is complying with both these mandates.

As a matter of background, ATS provides decision support functionality for CBP officers working in Advanced Targeting Units (ATUs) at United States ports of entry and CSI foreign ports. The system provides uniform review of cargo shipments for identification of the highest risk shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. ATS uses a rules-based program to highlight potential risk, patterns, and targets. Through rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air.

Working actively with the trade through the Departmental Advisory Committee on Commercial Operations (COAC), CBP has developed a new Security Filing in an effort to obtain additional advanced cargo information and enhance their ability to perform risk-based assessments prior to cargo being laden on a vessel overseas. The CBP proposal, better known as "10 plus 2" covers the following key areas:

- Ten unique data elements from importers not currently provided to CBP 24 hours prior to the foreign loading of cargo;
- Two additional data elements provided by the carriers including the Vessel Stow Plan, which is currently utilized by the vessel industry to load and discharge containers, and the Container Status Messaging, which is currently utilized by the vessel industry to track the location of containers and provide status notifications to shippers, consignees, and other related parties.

A Notice of Proposed Rulemaking (NPRM) is currently being developed. Obtaining additional information earlier in the process will increase the transparency of the global supply chain enabling the refinement of CBP's targeting processes and will provide additional information to make a more fully informed decision with respect to the risk of individual shipments.

In addition to Security Filing, CBP continually monitors the performance of weight sets and uses data analysis to modify rules and weight sets in ATS. Since 2004, ATS has undergone independent audits from the GAO and the IG. Furthermore, CBP regularly reevaluates to improve the data sets in ATS. The Office of Field Operations National Targeting and Security (NTS) office and the Office of Information Technology Targeting and Analysis Systems Program Office (TASPO) have been working together to enhance the ATS Maritime rule set capabilities for ocean cargo targeting. Under the direction of the office of field operations (OFO), TASPO placed the updated rule sets into production on March 21, 2007, to conduct initial assessments. Since that time, OFO subject matter experts and members of the Maritime Targeting Working Group have provided feedback to NTS, which resulted in further refinements and enhancements to the maritime rule set. Currently NTS is modeling several versions of the new Country of Interest list to include iterations of different scores and scenarios to include entity concepts such as first time, unknown, and high volume. OFO is currently using the updated rule set for maritime threshold targeting.

Customs-Trade Partnership Against Terrorism (C-TPAT)

Customs-Trade Partnership Against Terrorism (C-TPAT) is an integral part of the CBP multilayered strategy. CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C-TPAT has enabled CBP to leverage supply chain security overseas where CBP has no regulatory reach. Throughout 2007, CBP has continued to expand and strengthen the C-TPAT program and ensure that certified member companies are fulfilling their commitment to the program by securing their goods moving across the international supply chain to the United States. To carry-out this critical tenet of C-TPAT, teams of Supply Chain Security Specialists (SCSS) will conduct validations and begin revalidations of C-TPAT members' supply chains to ensure security protocols are reliable, accurate, and effective.

The SAFE Port Act not only legislatively recognized C-TPAT, but the Act also added greater accountability by mandating that certain program activities be completed within specific time frames, and that greater program oversight be developed for the program. CBP began implementing such changes, which were first outlined in GAO reports from 2003 and 2004, eighteen months prior to the passage of the Act and continues to make progress in this regard.

Specifically, clearly defined minimum security criteria have been developed and implemented for the major enrollment sectors and will be completed for all current enrollment sectors by this fall. The SAFE Port Act requires CBP to work with the COAC to review and modify as appropriate these criteria on an annual basis, and they have done so. This program enhancement will be completed each year as part of the development of the C-TPAT annual plan, another SAFE Port Act requirement. CBP is finalizing revisions to the C-TPAT Strategic Plan, which was first published in December 2004.

The SAFE Port Act also required CBP to review their certification processes for new members and make adjustments to strengthen this initial review if necessary. CBP has done so, and all new applications are being reviewed within 90 days.

Additionally, the Act requires that all new certified members undergo their initial validation within 1 year of acceptance into the program and be revalidated every four years. In 2007, CBP's goal is to complete 3,000 validations. As a point of reference, CBP completed 133 validations in 2003; 287 in 2004; 1,080 in 2005; and 2,398 in 2006. This is real progress, and it has been made possible by adding Supply Chain Security Specialists to the program.

With current staffing levels, the C-TPAT program should fulfill its operational goals for both the 2007 and 2008 calendar years. With the projected level of validations and revalidations needed to be in compliance with the Act set at just less than 3,000 per year, the current staff of 150 SCSS's should be able to manage this workload. The SAFE Port Act mandates that all revalidations must occur within 4 years of the initial validation, while the FY07 DHS Appropriations Act called for revalidations to occur within 3 years of the initial validation. Thus, the C-TPAT program is moving forward on a 3 year revalidation model to ensure compliance.

Projected revalidations alone will reach over 2,300 in 2009. The addition of Mexican Highway Carrier validations (done annually due to higher risk models) will add approximately 400. Further, required initial validations within 1 year of certification are being projected at 1,800. As a result, the final validation/revalidation totals needed would well exceed 4,000 for 2009 creating compliance issues with the current staffing numbers.

However, an additional staffing of 50 SCSS's will be brought on board with the creation of two new offices, one in Buffalo, NY, to focus principally on Canadian membership, and an office in Houston, TX, to focus on Mexican enrollment. With the addition of this staff, expected by early calendar year 2008, the C-TPAT would again see compliance with SAFE Port Act mandated timelines.

Working with COAC, CBP has also developed and implemented a pilot program using third parties to validate supply chains where CBP currently lacks full access. In May 2007, CBP selected 11 firms to act as validators in China as the Chinese government continues to deny access to CBP personnel wishing to conduct supply chain security validations. The Chinese Government has officially indicated that the matter is under review within their government, noting initially that the private sector in China may be reluctant to have C-TPAT validations conducted in-country. In an effort to show there was trade support for the process, CBP identified a certified C-TPAT partner that has significant business in China to demonstrate their willingness to participate in the validation process. Additionally, the CBP Commissioner and senior managers have traveled to China to discuss this matter with their counterparts in an effort to clarify the validation process as well as to offer a joint validation pilot involving five currently certified C-TPAT companies willing to participate. We have received no official response to this proposed project as of this date.

Interest in the pilot program has thus far been minimal. Of the more than three hundred (300) C-TPAT importers that were invited to participate in this voluntary pilot in June, less than a dozen importers have opted to do so to date. The primary concerns expressed by C-TPAT members for not participating lie in the sharing of proprietary business and security data with a third party and with the costs associated with the validation, which, as outlined in the SAFE Port Act, must be incurred by the C-TPAT member.

Container Security Standards and Procedures

CBP strongly supports and continues to seek opportunities to enhance supply chain security efforts, including enhancements to the security of the container. Indeed, securing the container is a critical part of a multi-layered approach to supply chain security. However, in order to establish minimum standards for container security, it is first necessary to ensure that there are available solutions that would significantly improve container security without significantly disrupting the flow of legitimate commerce. It should be noted that minimum security criteria for participants in the C-TPAT program do include a requirement that all C-TPAT importers must affix a high security seal to all loaded containers bound for the United States. These seals must meet or exceed the current ISO/PAS 17712 specifications for high security seals. C-TPAT membership currently accounts for 46% of total importations into the U.S.

Any technological solution would also need to be adopted as part of a broader supply chain security program. While CBP does not believe that, at the present time, the necessary technology exists for such solutions, CBP is working closely with the Department and is actively working with industry to test different technologies and methodologies that would provide economically and operationally viable enhancements to container security.

In-Bonds

The SAFE Port Act also required CBP to submit a report on in-bond cargo no later than June 30, 2007. CBP apologizes for the lateness of this report, which is still undergoing review, and expects to have the report issued shortly.

The final report includes a plan for closing in-bond entries at the port of arrival; an assessment of the personnel required to ensure 100 percent reconciliation of in-bond entries between the port of arrival and the port of destination or exportation; an assessment of the status of investigations of overdue in-bond shipments and an evaluation of the resources required to ensure adequate investigation of overdue in-bond shipments; a plan for tracking in-bond cargo within the Automated Commercial Environment (ACE); an assessment of whether any particular technologies should be required in the transport of in-bond cargo; an assessment of whether ports of arrival should require any additional information regarding shipments of in-bond cargo; an evaluation of the criteria for targeting and examining in-bond cargo; and an assessment of the feasibility of reducing the transit time for in-bond shipments, including an assessment of the impact of such a change on domestic and international trade. In addition, CBP is in the process of utilizing the evaluation of in-bond criteria to assist in the creation of a weight set for use in ATS to further assist in the identification of potential in-bond diversion cargo shipments.

CBP believes that the report is responsive to the concerns expressed by Congress, and a dedicated working group of experts has just concluded an in-depth review of the in-bond process and their recommendations will also address the report topics.

Office of International Trade

The mandates of the SAFE Port Act and the actions of CBP intersected again when CBP formed the Office of International Trade in October 2006. The establishment of this office serves to strengthen CBP's ability to carry out our mission of facilitating the flow of legitimate trade across U.S. borders while securing the borders and protecting the American economy from unfair trade practices and illicit commercial enterprises. The Office of International Trade consolidates trade policy, program development, and compliance measurement functions into a single office, providing greater consistency within CBP with respect to its international trade programs and operations. In addition, CBP's close working relationship with the trade community, a hallmark of CBP's operations and programs, has been further enhanced. The new Office of International Trade is providing CBP and the Trade community with an organization that can effectively address the growing volume and complexities of international trade and is enabling us to successfully meet the challenges inherent in managing the balance of trade and security.

In June 2007, to meet the Congressional requirements of the SAFE Port Act, CBP provided to Congress a resource optimization model (the "model") for the commercial operations and revenue function. The objectives of the model are to: (1) optimally

align the workforce to achieve management performance outcomes and goals; (2) adequately address risks inherent in the priority trade issues; and (3) comply with statutory requirements. The model has been designed to determine the right number and right mix of resources to facilitate legitimate trade while enforcing the trade laws.

Additionally, in preparation of submitting a report on the reorganization into the Office of International Trade, CBP has been meeting regularly with the COAC subcommittee on the Office of International Trade. During this first year, the subcommittee has been working together to find mutually beneficial process improvements to facilitate legitimate trade, which in turn will assist CBP in its trade enforcement efforts.

Conclusion

The steps that CBP is taking to implement the SAFE Port Act are and will be an extremely important aspect to the security of the nation. Through the SAFE Port Act, Congress has recognized and bolstered many of our aggressive programs to enhance security while assuring the facilitation of legitimate trade. We appreciate the close cooperative relationship the Department of Homeland Security and CBP had with the House and Senate in the development of the Act, and we look forward to the continued interaction to promote our mission and ensure the safety of American citizens and commerce.

Ms. SANCHEZ. I ask unanimous consent that Mr. Pascrell be allowed to sit and question at today's hearing.

Next, we will hear from Mr. Oxford to summarize his statement 5 minutes.

STATEMENT OF VAYL OXFORD, DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, DEPARTMENT OF HOMELAND SECURITY

Mr. OXFORD. Chairman Sanchez, Ranking Member Souder, Chairman Thompson, and other members of the committee, I would like to thank you for the opportunity to share the progress we have made in improving port and cargo security.

Keeping our Nation's ports secure is a critical layer in protecting our citizens against nuclear terrorism. The SAFE Port Act formerly authorized the establishment of DNDO, also identified a number of goals and reporting requirements for our Department.

I am happy to share that DNDO is meeting the requirements outlined in the SAFE Port Act. We have made excellent progress in deploying radiation detection technology at our busiest ports and land borders, resulting in the scanning of 94 percent of all incoming cargo into the United States.

Two years ago, only 40 percent of incoming containerized cargo was being scanned for radiological and nuclear threats. DNDO has worked closely with CBP to develop a joint RPM deployment strategy that balances risk against the measures of insuring the flow of commerce. RPM deployments to the Nation's 22 busiest seaports are complete. We are scanning over 95 percent of cargo coming through our seaports, using 374 radiation portal monitors. At select seaports, scanning now covers 100 percent and vehicles. By the end of 2007, 98 percent of all containerized sea cargo entering the United States will be scanned for radiological and nuclear threats.

Deployments to our land borders are also proceeding. There are 241 RPMs operating on the northern border and 353 RPMs operating on the southern border. This results in the scanning of 91 percent of containerized cargo coming across the northern border and 99 percent across the southern border.

As a result of this progress, we are meeting the mandates set forth in the SAFE Port Act that require that all containers entering high-volume ports by vessel be scanned for radiation. Also, the SAFE Port Act outlines five reporting requirements for DNDO. My written testimony covers the status of those reports, but suffice it to say, that we have met all reporting and requirements.

The SAFE Port Act also requires DNDO to establish an intermodal radiation detection center. There are several seaports that load cargo directly from ships to rail cars, bypassing the typical exit gates scanning operations used by CBP. Today we do not have a detector that can address this challenge. An intermodal rail test center will help develop additional passive detection systems that meet unique port requirements, thereby enabling DNDO to provide solutions that enable us to scan 100 percent of cargo containers entering the United States. The Port of Tacoma was chosen as the location of the rail test center because more than 70 percent of imported cargo through this port is handled by rail. We are working with the Port of Tacoma and CBP to begin operational testing associated with the intermodal rail concepts and evaluating technical solutions to fit the unique detection requirements of intermodal terminals.

I would also discuss additional port security efforts involving DNDO. These are not outlined specifically in the SAFE Port Act, but contribute to security in the maritime environment and for our country overall.

We are working with the Coast Guard to implement an acquisition plan in which DNDO develops and acquires systems for U.S. Coast Guard use. As a result, we will deploy radiation detection capabilities to every Coast Guard inspection and boarding team by the end of 2007. We also recently announced the West Coast maritime pilot that is beginning in the Puget Sound of Washington State and will expand into San Diego, California. The pilot will provide maritime radiation detection capabilities for State and local authorities with the goal of reducing risk of radiological and nuclear threats that can be illicitly transported on recreational or small commercial vessels.

This pilot program is being worked in close cooperation with the U.S. Coast Guard and CBP, as well as State and local officials. We expect to deploy human, portable, mobile, and fixed radiation detection systems as part of this pilot. We will also be working with maritime partners to assess the geographic configurations of the ports to maximize detection and interdiction opportunities. Maritime stakeholders will also receive guidance from DNDO on operational protocols, training exercises that support small vessel radiation interdiction operations.

In conclusion, port security is a critical component in protecting the U.S. from nuclear terrorism. The SAFE Port Act codified many of the requirements and strategies that will ensure a robust defense against threats to our Nation. The NDO and its partners have made significant progress over the last 2 years and will continue to make progress in keeping this Nation safe. I look forward to working with all of our partners in DHS, other departments, State and local agencies, and the members of this subcommittee as well as Congress in continuing the pursuit of this goal.

This concludes my prepared statements. I look forward to your questions.

[The statement of Mr. Oxford follows:]

PREPARED STATEMENT OF VAYL S. OXFORD

Introduction

Chairwoman Sanchez, Ranking Member Souder, and distinguished Members of the Committee, as Director of the Domestic Nuclear Detection Office (DNDO), I would like to thank you for the opportunity to share the progress we have made in improving port and cargo security. Keeping our Nation's ports secure is a critical layer in protecting our citizens against nuclear terrorism.

One year ago, the President signed the SAFE Port Act, which formally authorized the establishment of the DNDO. This important piece of legislation also identified a number of goals and reporting requirements for our Department. It helped ensure that we have the right security strategies in place and that we maintain our momentum as we implement protective measures.

I am happy to share that DNDO is meeting the requirements outlined in the SAFE Port Act. We have submitted a number of reports to Congress due earlier this year (including our comprehensive strategy for the deployment of radiological and nuclear detection equipment) and we expect to meet the deadlines for those that remain. We also have made excellent progress in deploying radiation detection technology at our busiest ports resulting in the screening of 93 percent of all incoming seaborne cargo into the United States.

Port Security Strategy

Before I go into more detail about the progress we have made in regards to the SAFE Port Act, I would like to explain our strategy at DNDO for deploying detection technologies to our Ports of Entry (POEs). Eighteen months ago, only 37 percent of incoming seaborne containerized cargo was being scanned for radiological and nuclear threats. DNDO worked in partnership with our colleagues at Customs and Border Protection (CBP) to develop a joint radiation portal monitor (RPM) deployment strategy that incorporates an optimized mix of current—and next-generation technologies, balancing our need for better capability with a desire for increased coverage against the associated costs of each. This joint strategy is predicated on placing next-generation systems, like the Advanced Spectroscopic Portal (ASP), at the highest throughput ports, where reductions to secondary inspection rates will have the greatest benefit. Deployment of ASP systems will be dependent upon the Secretarial certification of the systems as required by the FY 2007 Homeland Security Appropriations Act (P.L. 109–295).

Our strategy up to now has prioritized deployment activities based on risk, vulnerability, or consequence, as influenced by major populations, industries, importance to the economy and supply chain, or military bases located nearby. We also consider prior records of illicit activities. Finally, we consider whether locations had upcoming port reconfiguration.

We have taken steps to prepare for additional deployments and are conducting site surveys, developing site designs, and starting negotiations to award construction contracts for each of the crossings. As a general practice, DNDO works with the port authority to proactively schedule construction to coincide with any other activities at the port. This helps prevent scheduling delays and expedites the deployment process overall.

Our priority remains to finish deploying RPMs to high volume seaports and land border crossings. However, our future plans are addressing the hundreds of smaller crossings that dot the Northern and Southern borders, including rail crossings. We will also begin scanning of international air cargo.

Status of Deployments

RPMs have been deployed to all of the Nation's 22 busiest seaports. We are currently scanning 93 percent of cargo coming through our seaports using 358 RPMs. Moreover, at select major seaports, exit scanning now covers 100 percent of all containers and vehicles. By the end of this calendar year, 98 percent of all containerized sea cargo entering into the United States at the 22 busiest ports will be scanned for radiological and nuclear threats.

It is also important to mention deployments to our land borders. There are 241 RPMs operating on the Northern border and 343 RPMs operating on the Southern border. This results in scanning 91 percent of containerized cargo coming across the Northern Border and 97 percent coming across the Southern. In addition, a total of 60 RPMs are deployed to sites such as mail and express courier consignment fa-

cilities. By focusing on major ports of entry first, we have been able to dramatically boost the scanning levels of incoming cargo. We are also conducting scanning of privately owned vehicles (POVs). Our detection equipment currently scans 81 percent of POV traffic coming across the Northern border and 92 percent across the Southern.

Meeting the Requirements of the SAFE Port Act

Based on the progress we have made with RPM deployments at POEs, we are meeting the mandates set forth in the SAFE Port Act that require that all containers entering high-volume ports by vessel be scanned for radiation. In addition, we have developed the required strategy for the deployment of radiation detection capabilities, and that strategy has been submitted for the record as an amendment to this testimony. However, there are a number of other requirements outlined in the Act that we have been asked to fulfill and I would like to give you an update on each.

In total, the SAFE Port Act outlines five reporting requirements for DNDO. Our deployment strategy was submitted first to Congress in March 2007 and included information on a risk-based prioritization of ports, a proposed timeline for deployment, the types of equipment that we are proposing for each port, documentation of standard operating procedures for examining containers, operator training plans, and the Department's policy of using non-intrusive imaging equipment. As I mentioned earlier, one aspect of our joint deployment plan with CBP is how we plan on introducing next-generation technologies like ASP into the field. Right now, ASP is pending Secretarial certification and will not be fully deployed until that certification process is complete. If the outcome of the certification process is positive, we will submit an amendment to our strategy to identify the locations at which we will deploy ASP. The report also included a classified annex that details plans for covert testing of the top 22 seaports, as required by Section 121 of the Safe Port Act. The DNDO Red Team is working with CBP to build and maintain documentation of these activities.

Secondly, in April 2007, we submitted a joint report with the Science and Technology Directorate, CBP, and DHS Office of Policy Development that outlined the feasibility of and strategy for development of chemical, biological, radiological and nuclear (CBRN) detection equipment. DNDO submitted content that clearly documented both near- and long-term research and development efforts that will provide improved nuclear detection capabilities.

The third report required that DNDO, along with CBP, complete an evaluation of health and safety issues related to the use of non-intrusive imaging (NII) technology to scan containers. DHS fully understands the environmental health and safety impacts of NII technology. DHS has a comprehensive radiation risk reduction plan, and will continue to work closely with the Nuclear Regulatory Commission, Occupational Safety and Health Administration, and the National Institute for Occupational Safety and Health to minimize radiation exposure of workers and the public to levels as low as reasonably achievable. Additionally, DHS will continue to monitor environmental health and safety impacts associated with NII technology by constantly addressing these impacts with systems currently deployed and systems under development. As next-generation NII systems are developed, DNDO will make a constant effort to address environmental health and safety issues by consulting with the National Council on Radiation Protection and Measurements, and conducting modeling and benchmarking. This report was submitted in July 2007 and received no comments from Congress except for a request to make our findings open for distribution to the private sector. We complied with this request and modified the document so that it was no longer For Official Use Only (FOUO).

The two remaining reports, an overall investment strategy for radiological and nuclear detection across the US government, and a report on how DNDO authorization language impacted the Homeland Security Act of 2002 and DHS research and development efforts to detect, prevent, protect, and respond to chemical, biological, radiological, and nuclear terrorist attacks, are scheduled to be delivered in October. We are working with other DHS components and across the interagency to ensure that these reports are comprehensive in nature and delivered to Congress in a timely manner.

The SAFE Port Act also required DNDO to establish an Intermodal Rail Radiation Detection Test Center. This was a very forward thinking requirement and one that DNDO strongly supports. There are several seaports that load cargo directly from ships to rail cars, therefore bypassing typical exit gate scanning operations. Right now, we do not have a detector that can address this challenge. An intermodal rail radiation detection test center will help develop additional passive detection design variants that meet unique port requirements, thereby enabling DNDO to pro-

vide solutions that enable us to scan 100 percent of cargo containers entering the United States. The test center was announced in May of this year and was awarded to the Port of Tacoma, Washington. The Port of Tacoma was chosen as the location of the Rail Test Center because more than 70 percent of its total import cargo volume is handled by rail at its multiple intermodal rail terminals. We are working diligently with the Port of Tacoma and CBP to begin testing the operational needs associated with intermodal rail, as well as evaluating innovative technical solutions to fit the unique radiological and nuclear detection requirements of intermodal terminals.

Additional Port Security Efforts

I wanted to take the opportunity today to also discuss additional port security efforts in which DNDO is involved. These are not outlined in the SAFE Port Act, but contribute to security in the maritime environment and for our country overall.

DNDO has an excellent working relationship with our Coast Guard operators. We have a joint acquisition plan in place that will allow DNDO to both develop and acquire systems for USCG use. DNDO provided handheld and backpack radiation detection devices to fulfill imminent operational needs in fiscal year 2007. We will deploy radiation detection capabilities to every Coast Guard inspection and boarding team by the end of 2007. The Secretary stated that this is one major goal for this Department, and we are going to meet that goal. We are also developing next-generation technologies that have the identification capabilities, connectivity, and ruggedness required in the maritime environment.

We also recently announced the West Coast Maritime pilot program that is beginning in the Puget Sound region of Washington State and will expand into San Diego, California. The three-year pilot will provide maritime radiation detection capabilities for State and local authorities with the goal of reducing the risk of radiological and nuclear threats that could be illicitly transported on recreational or small commercial vessels. We will be conducting this pilot program in close coordination with the U.S. Coast Guard and Customs and Border Protection. DNDO expects to deploy non-intrusive, passive detection sensors, such as human-portable radiation detection equipment, mobile sensors, and fixed-position detectors. We will also be working with maritime partners and local authorities in both areas to assess the geographic configurations of the ports to maximize detection and interdiction opportunities. Additional analyses for local partners will include a baseline survey of the existing radiological and nuclear detection architecture, a gap and risk assessment, and associated recommended actions to be developed in conjunction with maritime stakeholders. Maritime stakeholders will also receive guidance from DNDO on operational protocols, training, and exercises that support small vessel radiation detection capabilities.

Conclusion

The mission of the DNDO reaches far beyond port security. However, port security is a critical component in protecting the U.S. from nuclear terrorism. The SAFE Port Act codified many of the requirements and strategies that we will ensure a robust defense against threats to our Nation. The DNDO and its partners have made significant progress over the last two years, and will continue to make progress in keeping this Nation safe. I look forward to working with all of our partners within DHS, other departments, State and local agencies, and the members of this subcommittee and Congress in continuing to pursue this goal.

This concludes my prepared statement. Chairwoman Sanchez, Ranking Member Souder, and Members of the Committee, I thank you for this opportunity and would be happy to answer any of your questions at this time.

Ms. SANCHEZ. I now recognize Mr. Caldwell to summarize his statement in five minutes.

Mr. CALDWELL. Madam Chairman, Mr. Souder, and also Chairman Thompson, thank you very much for inviting me back 6 months after your initial hearing on the SAFE Port Act. Not only has it been a year now since the SAFE Port Act was enacted, but now we are approaching the 5-year mark on the enactment of MTSA which, as you know, really created the framework for maritime security that the SAFE Port Act actually enhanced.

Given the breadth of the SAFE Port Act, the statements of the other witnesses, and my already submitted lengthy statement, I

think I am going to focus my oral comments on two areas. One is interagency operation centers, and the other is port recovery issues.

Regarding interagency operation centers, as you know, the SAFE Port Act required the establishment of these centers. In 2003, let me give you a little history, Congress appropriated \$50 million for Project Seahawk in Charleston Harbor. This was designed as a program that would take different agencies and different technologies and try to combine them to prevent and deter terrorist attacks at least in Charleston. About that same time, in 2003, in the wake of the U.S.S. Cole attack, as well as the 9/11 attack, the Navy was looking for a way to help protect its ships that were in homeport in the U.S.

They partnered with the Coast Guard to develop something called Joint Harbor Operations Centers, or JHOCs. There is one of these originally in San Diego and in Hampton Roads. Then finally, also about that time in 2003, Coast Guard began a reorganization to combine some of its operational units with some of its marine environmental and safety units, and combining these into something called sectors and started developing sector command centers. The important difference between Seahawk and JHOC and the sectors was that the Seahawk and the JHOC centers were really focused exclusively on maritime security whereas the sector command centers in some ways leveraged resources further in focusing on the wide variety of Coast Guard missions that would be included, such as in search and rescue, protection of fisheries, all the other missions the Coast Guard sector would have. The Coast Guard now reports that it has sector command centers in all 35 of its sectors, and the SAFE Port Act has then required DHS to establish something called interagency operation centers at high-priority ports within three years. DHS has provided Congress with a plan, a five-year plan to upgrade these current sector command centers into interagency operation centers at 24 ports and estimated the cost at \$260 million.

Moving forward on these operational centers, we found there is a couple of challenges ahead for Congress and for the Executive Branch. One is the obvious resource question. While there is an estimate of \$260 million, those funds have not been identified or appropriated. In addition, every port is different and I think we have all heard that deal with ports, and so there needs to be clear roles and responsibilities among the multiple agencies. I think for the Coast Guard the roles and responsibilities are fairly clear, but at different ports you have several other important stakeholders, whether they are the Navy or Customs or other state and local stakeholders. And, finally, one of the issues we have identified in the past that is not completely resolved is the issue of security clearances for all appropriate stakeholders.

Moving on to recovery. The SAFE Port Act asks for more emphasis in both plans and exercises on recovery issues. Going back to MTSA, MTSA required that there be security plans in every port, every major port at least, and the Coast Guard has implemented those with general guidance. However, our review of these plans found that the guidance was fairly vague in terms of recovery issues.

While there is some national level guidance in terms of the national maritime infrastructure recovery plan, those plans as well as the exercises associated with them need to be focused more at the port level. And the Coast Guard has taken steps to do this, but I think as Captain Sturm has mentioned, some of these will not be in place until these individual port plans are revised by July 2009.

With that, I would like to close out my statement. And be happy to answer any questions. GAO will continue to work with this committee and others in Congress to provide oversight over the SAFE Port Act to best practical port security for our Nation. Thank you.

[The statement of Mr. Caldwell follows:]¹

Ms. SANCHEZ. I thank all of our witnesses for their testimony.

I will remind each member that he or she will have 5 minutes to question the panel. And I will now recognize myself for a couple of questions.

On your testimony, Mr. Caldwell, you said that the Coast Guard had general guidance, under general guidance. From whom?

Mr. CALDWELL. The Coast Guard's guidance came out in the form of a NAVIC, correct me if I am wrong, Captain, but that is Navigation and Vessel Information Circular, providing some guidance on what each area maritime security plan should have. And this went out to the committees when they first developed their plans in 2004.

Ms. SANCHEZ. Thank you for that clarification.

I would like to ask Mr. Winkowski, this has to do with C-TPAT, a program that I am particularly interested in. The pilot program that was included in the SAFE Port Act was to provide additional validation options at a time when CBP was unable to perform enough validations; they had gotten behind. It is interesting now to me, and I am pleased that we have been able to validate a majority of the C-TPAT members security plans, I think, also because we provided some additional personnel to be able to do that.

So my question is, do you believe that there are still third-party validation processes which would be useful? In other words, do we still need them? Are we going to stay full up and continue to do these reevaluations at least once every four years with just the personnel? Or do you think that there is still room for this third-party validation process to exist?

Mr. WINKOWSKI. Well, first, I would like to thank the committee for being so generous with the C-TPAT program. We have a full complement of staff on. We have increased it. We have opened up offices in Buffalo and Houston as well, and that has enabled us to move along quickly to validate. I think it is too early to tell on the third-party validators.

As I mentioned in my opening statement, only nine importers have signed up, and 11 validators were selected. To my knowledge, they still have not been able to do the validations. It has to do with pricing, it has to do with an individual's willingness to want to hand over sensitive trade related information.

¹ See GAO, "MARITIME SECURITY: The SAFE Port Act: Status and Implementation One Year Later", Tuesday, October 30, 2007, GAO-08-126T.

So I am optimistic, Chairwoman Sanchez, that at some point here in the not so distant future, that China will open its doors and our team will be able to go in there and do the validations.

Ms. SANCHEZ. On the pilot, you chose as the universe for third-party validators to look at only members, only C-TPAT members with 75 percent or more of their supply chain in China. I think that this would result in a small number of potential universe for these third-party validators to actually take a look at. I am told something around 300 eligible. What made you, what made you choose that particular 75 percent figure?

Mr. WINKOWSKI. There was an analysis done based on threat and other factors, and we came up with the 75 percent figure.

Ms. SANCHEZ. Because of threat factor?

Mr. WINKOWSKI. Threat, trade volumes, things of that nature. And from there we came up with that 75 percent number.

Ms. SANCHEZ. Okay. I have heard also that the supply chains in China aren't considered very risky in the C-TPAT program. How do we know that if we have never actually been allowed to go in and look at the supply chain?

Mr. WINKOWSKI. C-TPAT was set up from a terrorist standpoint, and we have had no information that China is a threat from that standpoint.

Ms. SANCHEZ. We have no information that China is a, has terrorists who would be wanting to go from there in hurting our commerce or our people?

Mr. WINKOWSKI. That is correct.

Ms. SANCHEZ. Okay. What is the status of the negotiations for China to allow our CBP validators to go into China?

Mr. WINKOWSKI. We are waiting for a letter from the Chinese government that we anticipate getting at any time now to open up the doors. And we have already selected team members. Our C-TPAT supply chain specialists have been selected. And as soon as we get that letter and they open the doors, we will be in there beginning the validation process.

Ms. SANCHEZ. When we go to other countries and look at the C-TPAT and do the validations, is that a long-term situation where we put employees there, or do we just house them in hotels, they go and do it for a week's time?

Mr. WINKOWSKI. They stay in hotels. They are not permanently stationed there. Depending on the size of the supply chain, it depends on the size of the supply chain and determines how long they would be there.

Ms. SANCHEZ. I see that my time is up. So at this moment, I will yield 5 minutes to the ranking member for his questions.

Mr. SOUDER. Mr. Winkowski, if North Korea wanted to move something through the United States, would they likely use China?

Mr. WINKOWSKI. I don't know.

Mr. SOUDER. Seemed a fairly broad statement to say that we have no concerns about China, given the amount of shipments that we have go through there. I think you accurately stated that we haven't any publicly released incidents. But I think there is grave concerns about even whether China can call Western China, as their Muslim population, where things may move through their

ports. Malaysia clearly has people moving every which direction and Indonesia and the Philippines.

Mr. WINKOWSKI. But from the supply chain standpoint, China's threat is clearly more on the import safety side of it.

Mr. SOUDER. I understand that, given the bulk that that is true, but I don't know that I agree with your underlying assumption. I wanted to ask you and Mr. Oxford the statement that the SAFE Port Act includes a list of criteria that has to be evaluated, and I know a lot of this is relatively new. But we ran into this last week on our border implementation, and so I want to go through the list of things that you have to give feedback before you roll this out. One was the ability of the automated targeting system to utilize the images and the data capture during the scanning, which is one of the problems that we have had in the borders, is that we get the info but we don't know how to handle it.

The second is the effectiveness of the scanning equipment in detecting shielded and unshielded nuclear material. In other words, can we see actually what we are trying to see. The ability of the software to automatically identify potential anomalies in scanned containers, for years this has been a challenge in narcotics and other types of things and I have seen many variations both overseas and in the United States. The feasibility of expanding the pilots to other ports, including available infrastructure, processing speed, cost to install and maintain, and the number of staff required. And I am wondering if each of you could give us a preliminary on those four key points.

Mr. OXFORD. The problems that you have stated with scanning in the past, especially the imaging as opposed to the passive scannings, is something that technology will quickly advance. What we are working with CBP to do is to look at the various scanning systems that are out there and find out the information content that comes in each one of those scans. What we have been doing in the past or what CBP is doing at the borders, if you have visited there, is essentially doing a manual processing of the imaging, and then they are trying to make a determination integrating automatic algorithms into that scanning process to immediately alert the operator there is an anomaly, is the technology within our grasp. What we need to identify are the systems that we can now integrate that technology or that capability into to further enable the CBP officers as they are trying to make these targeting systems.

So, from a technology point of view, it is within our grasp. We need to find the right systems to integrate the automated processing piece of this, which has not been a requirement in the past. So this is a new requirement that needs to be integrated in the imaging systems.

Mr. WINKOWSKI. And we work very closely with DNDO on that.

Mr. SOUDER. Have you been able to position the images themselves? Is what you are bringing in, for example, being able to be used by the National Targeting Center?

Mr. WINKOWSKI. Yes, they are. As a matter of fact, I was at the Center yesterday. And when you look at Pakistan, the images are very, very clear that are being transmitted out of the SFI port.

Mr. SOUDER. Thank you.

Mr. Oxford, I appreciate the time that we spent earlier talking about a number of these issues. And one of the things that has been a question is how you do a cost benefit analysis of your new technologies. Could you explain a little bit some of the struggles that you have had those, the tradeoffs you have had and the costs and the expensiveness versus the return?

Mr. OXFORD. The trade-off boils down to two principle factors. First of all, is the technology providing a significant enough increase in performance to warrant the cost of that system? It also then gets back to the balance that I mentioned earlier where we are trying to manage the threat. And, again, without going into our threat basis in terms of the amount of material we are trying to scan for domestically, it is a fairly low number and I won't go into the depth on that. But that trade-off between that and what CBP officers have to do at every port of entry becomes the principle factors in our cost benefit analysis.

How much time does it take to go through a current protocol, versus the benefit that new technology, while managing the threat better, also benefits the operators in terms of their performance.

Mr. SOUDER. When you are dealing with potential catastrophic threat that you are dealing with, how does that change a normal calculation as opposed to risk of illegal immigration, risk of narcotics, risk of patent violation? Nuclear is a whole different standard.

Mr. OXFORD. When you look at traditional cost benefit analysis, one of the methodology factors is the cost of regrets. So if you factor in the prospect of allowing a nuclear weapon into one of our major urban areas, the associated costs that could run into the trillions immediately suggests that you would pay whatever it takes to provide enhanced security at the border regardless of what the technology costs.

Mr. SOUDER. Okay.

Ms. SANCHEZ. I thank the gentleman for that.

And I would now like to recognize other members for questions that they may wish to ask the witnesses. And in accordance with our committee rules, I will recognize members who were present at the start of the hearing based on seniority on the subcommittee, alternating between the majority and minority. And those members coming in later will be recognized in order of their arrival, and of course, those members who are not traditionally on the committee will be recognized after that point.

So at this point, I would like to recognize the gentleman from Mississippi, our chairman, Mr. Thompson, for 5 minutes.

Mr. THOMPSON. Thank you very much, Madam Chairwoman, for this very important hearing. As has already been said, we have been talking about TWIC for about 5 years now. Ms. Fanguy, can you tell me if you are aware of the Coast Guard's advisory stating that criminal elements were trying to obtain the information about the TWIC program in the Ports of Los Angeles and Long Beach?

Ms. FANGUY. Yes, I am. And we have been working very closely with the Coast Guard to look at that intelligence.

Mr. THOMPSON. We will go into that a little more. The TWIC card was supposed to be the one card that provided uniformity and

consistency. What steps has TSA taken to pre-empt state access cards like those issued in Florida?

Ms. FANGUY. The TWIC regulation currently does not preempt States or localities from issuing their own cards. In the case of Florida, however, we recently participated in a roundtable chaired by Congressman Mica to discuss some of the concerns of the state of Florida and to identify ways that we can work more closely together so that we can have one card.

Mr. THOMPSON. So are you giving us testimony that at some point it is the Department's hope that all these other access cards will go away and this TWIC card will be the single entity that employers, and employees will have to use?

Ms. FANGUY. Everybody who needs unescorted access to the Nation's ports and vessels will require a TWIC. But currently, it is up to local business operators and States and local officials to determine if additional cards are required. But everybody will have a TWIC, which will provide a common and uniform credential across the entire maritime mode. And we feel that adds significant security benefits.

Mr. THOMPSON. But you are aware that if each State develops an access card, we have created a real problem for the employees.

Ms. FANGUY. We certainly have heard from a number of our stakeholders about the challenges that they face with multiple credentials. And that is why we are putting out the TWIC card, which is a common and consistent credential used nationally.

Mr. THOMPSON. And I appreciate your comments. But if 10 States decide to have their own access card, that means that a potential employee would have to have 10 access cards if they operate in those areas plus a TWIC card.

Ms. FANGUY. In the example you give, that is correct. And we are hoping that people will embrace the TWIC credential. And the way that we have designed it is that you can integrate it within many legacy systems in a lot of different ways. So we are hoping that the flexibility will allow people integrate it easily into their existing systems.

Mr. THOMPSON. Are you aware of any instances where the rollout at this point has produced any compromising of the TWIC card?

Ms. FANGUY. Not at this point.

Mr. THOMPSON. Can you tell us, according to the witness who will be only next panel from the Port of Houston, why the Department missed the estimated number of employees by more than 90 percent?

Ms. FANGUY. In terms of any port in the Nation, we certainly have heard a number of different estimates. Let me assure you that no matter how many workers there are, we are ready to take them. We have a flexible approach to be able to handle whatever volume comes our way. As an example, in the Ports of Los Angeles and Long Beach, we can do 24 by 7 enrollment. That is a 24 by 7 port. In places like Houston, where there are large populations, we are working very closely with field personnel to identify where some of the discrepancies may lie and to make sure that we have the resources there to be able to handle large volumes of workers.

Mr. THOMPSON. So, now, did the Department come up with these numbers internally? Or did we hire somebody to give us the estimates?

Ms. FANGUY. When TSA began developing the regulations for the TWIC program with the Coast Guard, we did extensive analysis. We worked to try to obtain numbers from trade associations, from labor groups. We worked with the Department of Labor. And we looked to all the various sources of data that we had available to us to identify the overall population estimates. But we continue to work closely with local stakeholders to make sure that if there is new information, that we take that into account and we have a flexible approach to be able to handle any group of workers that come our way.

Mr. THOMPSON. I understand. But what I was trying to say, was did we pay somebody to come up with these estimates, or did the Department internally come up with the estimates?

Ms. FANGUY. It was a Department-led initiative, and I am sure that we had contractor support. So we need to get back to you with some of the details if you are interested in more information.

Mr. THOMPSON. So you are not aware of any contract that went out to give the Department the estimated number of people who will be eligible for the TWIC card?

Ms. FANGUY. Again, it was a Department-led initiative. But I do know the way contractors support, but in terms of the statement of work specifically for that, we need to get back to you with those specifics.

Mr. THOMPSON. So do you know about any of the contracts?

Ms. FANGUY. Absolutely. The contract that supported the population estimates, I apologize it was before I was actually hired at the TSA, so I want to make sure to get you the right information, and I am sure we can get that for you as soon as we are done here.

Mr. THOMPSON. Thank you. Will you please get us that information?

Ms. FANGUY. Sure.

Ms. SANCHEZ. I will now recognize Mr. Bilirakis for 5 minutes.

Mr. BILIRAKIS. Thank you. And I want to thank the chairman for zeroing in on the TWIC card issue. We simply cannot require maritime workers in Florida or any other state to obtain multiple cards for the same purposes.

I want to commend you, Ms. Fanguy, for your willingness to work with me, my state's congressional delegation, also leaders from the Florida legislature on this particular issue. I hope by working through these issues that we can come to a mutually acceptable solution to improving port security in Florida and throughout the country.

I have a couple questions for you, Ms. Fanguy. I understand that just a few hours ago TSA released a quarterly deployment plan which indicates that TWIC enrollment is scheduled for most Florida ports in the first three months of next year. Do you know when TSA will be announcing specific enrollment dates for those particular ports?

Ms. FANGUY. As we get started on the program, we began in Wilmington. Once we verified that things were going successfully in Wilmington, we put out the date for Corpus Christi. So on Thurs-

day we are looking forward to getting the real data back, and then we will announce a lot more dates. So as we go through the next couple of months here, I would anticipate that we would begin to put out further information with specific dates and locations for the upcoming ports. But we want to do this in a measured way and we want to make sure to control the release of information so we don't confuse workers, and all of a sudden, have workers show up at an enrollment site only to be turned away if we have not begun enrollment in that location. But I would anticipate that that would be coming very shortly after we verify successful operations in these first ports.

Mr. BILIRAKIS. At a roundtable discussion on the TWIC last week, as you mentioned, former DHS Deputy Secretary Michael Jackson indicated that he believed that several of the outstanding TWIC issues could be resolved before TWIC is implemented in Florida. Could you please share with us what steps your office is taking to address the major unresolved issues and whether you have established a timetable for doing so, especially in light of today's deployment announcement.

Ms. FANGUY. We are working very closely within the Department of Homeland Security to take the feedback from that roundtable, and we have developed a plan. We are working very closely with the FBI to identify ways that we can make sure that at the national level, that we have access to complete criminal history records information that will allow us to complete more accurate security threat assessments. We have also prepared a letter to go to the FBI so that we can identify other ways that we can work more closely to address some of the issues that were brought up in the roundtable.

Ms. FANGUY. We have been working very closely with officials in the State of Florida, and I anticipate that we are going to continue to do that as we move forward with TWIC rollout to make sure that we have come up with a mutually agreeable solution.

Mr. BILIRAKIS. At the discussion, Secretary Jackson also said that he would also inform his successor about the discussions we had last week and direct him or her to make resolving the issue a top priority. Will you commit to me here today that will ensure that the Acting Deputy Secretary Snyder is aware of Florida's concerns and that he or she, the successor, will follow through on Secretary Jackson's promise in a timely manner?

Ms. FANGUY. Absolutely. And, in fact, he was already briefed and we gave him further information when we met with him last week to bring him up to speed on some of the issues that we discussed.

Mr. BILIRAKIS. This is very critical to Florida, so thank you for your cooperation and your willingness to continue to work for me. Thank you.

Thank you, Madam Chair.

Ms. SANCHEZ. The gentleman from Florida is welcome.

I believe now we have the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Madam Chair; and I thank the witnesses for appearing today. Because time is of the essence I will move as expeditiously as possible.

Ms. Fanguy or Fangee? Help me with the pronunciation.

Ms. FANGUY. It is Fanguy, but I will answer to almost anything.

Mr. GREEN. Thank you. I want to be as appropriate as possible.

Permit me to retrace some of the comments made. You indicated earlier that it would take approximately 15 minutes as an enrollment time and about a 6-minute wait period; is that correct?

Ms. FANGUY. That is the data that we are seeing to date.

Mr. GREEN. And you might be able to enroll as many as 5,000 workers per day?

Ms. FANGUY. That is correct, once we are rolled out nationwide.

Mr. GREEN. At 147 sites?

Ms. FANGUY. Correct.

Mr. GREEN. Now obfuscation does not necessitate malice aforethought, and I do not in any way imply that there is any malice aforethought, but I do have to ask you, are you indicating to us that we now have a working paradigm that we can monitor and that we can review wherein the card which necessitates that you have two things to happen, a reader that can read the card and can also read some part of my body so as to cross-check? Are we saying that that system is operable today?

Ms. FANGUY. Yes.

Mr. GREEN. And it is operable at 147 sites?

Ms. FANGUY. In terms of—there are two parts to the TWIC program. So, right now, we are moving forward with the rollout of enrollment of workers. And then the second part will be to require owners and operators at those ports to install readers.

Mr. GREEN. I understand, but do we have the readers at these sites?

Ms. FANGUY. Currently, they are not required to have readers.

Mr. GREEN. Is your answer no?

Ms. FANGUY. That is correct. It is no.

Mr. GREEN. If we do not have readers at the sites, then we will have persons who will have cards who will be permitted to enter a facility, but we won't have the ultimate cross-check, which is the reader that will identify the person as the proper holder of the card; correct?

Ms. FANGUY. Correct.

Mr. GREEN. That would mean then today I could take someone else's card who looks a lot like me—not a lot of people do, but assuming there is someone who looks a lot like me—and I could enter the facility—"thank God" someone just said. I could enter the facility with someone else's card if the person looks a lot like me; is this correct?

Ms. FANGUY. We would hope that the security officials at the port—

Mr. GREEN. I understand, but you don't have that crucial element of the cross-check with some biometric; is that correct?

Ms. FANGUY. That what we are working very closely on in the rollout—yes, the readers.

Mr. GREEN. The reason I mentioned obfuscation is because the way your testimony came across could cause someone to conclude that we have sites currently operable where this actual functionality is taking place and you are saying to me this is not true?

Ms. FANGUY. We have enrollment sites that are open, and the next part of the program will be to require readers.

Mr. GREEN. Which makes my statement correct then. You don't have the sites with the reader and the enrollment card?

Ms. FANGUY. For the readers, you are correct.

Mr. GREEN. Which means we are still at a point where we are—to use the vernacular of Texans—we are fixin' to do something. True?

Ms. FANGUY. Well, the first part of the program needs to be to get cards in the hands of workers so that then when you implement readers that everybody has a card. So we don't want to put a lock on the doors until everybody has a key, and what we are doing now is giving everybody the key.

Mr. GREEN. So you are 100 percent confident that the reader that you will eventually utilize will function with the card that you have developed?

Ms. FANGUY. When we developed—

Mr. GREEN. I might have to ask you to say yes or no, given that I only have 55 seconds left.

Ms. FANGUY. Yes, I am confident that we will have the—that we will be able to read the cards.

Mr. GREEN. One hundred percent confident?

Ms. FANGUY. Yes.

Mr. GREEN. The delay in getting the TWIC card developed and on line, would the vacancies in DHS have played any part in the implementation of the SAFE Port Act? Not just of the card but would these vacancies have had any impact?

Ms. FANGUY. Since I have been at the TSA, I was actually hired to take things forward with TWIC about a year and a half ago. We have hired additional staff to be able to move forward with the TWIC program, and we feel that we have a good staff in place to carry the program forward and continue successful operations.

Mr. GREEN. And I will take that as a nebulous answer, and I am not sure whether you said yes or no. Could you kindly give me some clarity, please? Are you saying yes or no?

Ms. FANGUY. I am not aware of any of the vacancies affecting the TWIC program.

Mr. GREEN. I will yield back the balance of my time with this comment. I am somewhat disappointed that after 5 years we still don't have the readers and the cards being dispatched. That causes me some degree of consternation, given that this is a key element in the SAFE Port Act.

I yield back.

Ms. SANCHEZ. I thank Mr. Green, and now we will go to Ms. Jackson Lee for 5 minutes.

Ms. JACKSON LEE. Let me thank the witnesses for their testimony and as well for their service and express the same kind of concern. I won't use the terminology "frustration" but "concern." Because I do believe that there has been an effort to move forward, by the witnesses' testimony. But, at the same time, I think that we are long overdue in where we should be.

Let me ask a pointed question to Ms. Fanguy and to the Commissioner. This program was supposed to be rolled out on January 1, 2008—I know in your testimony you have said a number of

things—at the top 20 to 50 ports. Give me your best answer that you will in fact be able to roll this program out at the top 20 to 50 ports January 1, 2008, which is a short distance away from today.

Ms. Fanguy, why don't you start?

Ms. FANGUY. Today we put out a schedule; and by January 1, 2008, we are currently anticipating that we will be at 39 sites. In January to March of next year, we are currently anticipating 55 more sites being brought on line and quickly bringing on the remaining 147 sites, so that by next September we would anticipate that we would have the full complement of fixed enrollment sites.

Ms. JACKSON LEE. Let me stop you there. You will have 39, which is between 20 and 50. And why do you think you are not able to do the complete 50 by January 1, 2008? And will the 39 that you have, will it meet the litmus test? Will you be comfortable that it will be a functioning process, the ones that you will have at that point?

Ms. FANGUY. That is exactly why we are rolling it out the way that we are. We want to make sure that we roll this out in a measured way and a controlled way to make sure that it continues to work successfully, that we can handle the volumes and continue to turn cards around in a timely fashion.

Ms. JACKSON LEE. We have listed as one of the problems that the Department has not yet finalized a rollout schedule for all the ports. Are you suggesting that there is finalized schedule and it is not a problem anymore?

Ms. FANGUY. We do have a finalized schedule that we have put out, and we will continue to put out more information about specific dates for each port as we move forward in the program.

Ms. JACKSON LEE. Let me hear that again. You said what?

Ms. FANGUY. We have a working schedule, and today what we have put out is time frames for the 147 ports. So for the next couple of month up to the end of December we have given time frames, but we need to make sure that we are verifying success at each port before we put out the dates for the next ports, because we don't want to have a situation where we announce a date for workers at a certain port and then we have to change those dates.

Ms. JACKSON LEE. Mr. Commissioner, why is this taking so long? And the second question is, why did you choose China in this pilot program? Why is this whole process taking so long?

Mr. WINKOWSKI. Congresswoman, I have nothing to do with TWIC. It is not under Customs and Border Protection.

Ms. JACKSON LEE. Then answer the question. You are still a part of the Department. I am sure you can contribute to that. Why did you select China as a pilot program?

Mr. WINKOWSKI. I am sorry. I thought you were talking about TWIC. From the standpoint of the third-party validators?

Ms. JACKSON LEE. Yes.

Mr. WINKOWSKI. China was picked due to the fact that the Chinese government would not let us in China. And so going by the SAFE Port Act and going by the requirements of the SAFE Port Act China was selected, hoping that we could get some C-TPAT validations completed.

Ms. JACKSON LEE. But you picked a nation that wouldn't let you in? I am trying to understand that.

Mr. WINKOWSKI. We had some issues from the standpoint of doing our validations there, and we felt that in order to help out the importers that wanted to be under the C-TPAT program that the third-party validators could perhaps move it along.

Ms. JACKSON LEE. Are you where you need to be with China now?

Mr. WINKOWSKI. No, we are not, but I am hoping in the next few days that we will be notified by China that our C-TPAT supply chain specialists will be able to go into China and begin the process of validations.

Ms. JACKSON LEE. I appreciate the service of everyone, but the question I posed to the commissioner was purposeful. It seems that no one at DHS knows what the other person is doing and has no contribution to it and can't help anyone. I will just make the point that coordination is lacking.

I have some other questions, but I know that my time is over. Thank you.

Ms. SANCHEZ. I will now recognize the gentleman from Texas, Mr. Cuellar, for 5 minutes.

Mr. CUELLAR. Thank you, Madam Chair.

I want to thank the witnesses for being here.

Commissioner Winkowski, let me ask you about the primary goal of the SAFE Port Act. It is the improvement of risk targeting for maritime cargo containers inbound to the United States from overseas locations. What is the status of the 10 plus 2 initiative?

Mr. WINKOWSKI. The 10 plus 2 initiative, the regulations have been forwarded up to the Department and OMB for further review and approval. So I think when you look at 10 plus 2, I think it is really testimony to how government and industry can sit down, take on a very difficult issue and come up with a solution.

Mr. CUELLAR. So your best timetable is by when?

Mr. WINKOWSKI. Hopefully, sometime—I am anticipating sometime this calendar year.

Mr. CUELLAR. What about the global trade exchange, the GTX initiative? What is the status of that?

Mr. WINKOWSKI. We continue to work through that. It is an initiative that we have had a series of meetings on. It is a data warehouse. It is a vision that we have. Our attorneys are going through the legal challenges that we have with the global trade exchange, and we continue to move along.

Mr. CUELLAR. Have you all included the custom brokers, the industry? I talked to their association, and they feel quite strongly that they have been left out of the conversation.

Mr. WINKOWSKI. Not at this point, Congressman, because it is really something that we are trying to get our arms around. But I can assure you that once we get our arms around it and issue the RFQ that there will be very, very strong consultation with the trade community.

Mr. CUELLAR. Okay. So when you do get your arms around that you will still have flexibility to—if they would want to see some changes, you would have flexibility to make any changes from the input?

Mr. WINKOWSKI. Oh, yes.

Mr. CUELLAR. Let me ask you a question about the container security devices required under the SAFE Port Act. Have you all developed any container security devices required by the Act?

Mr. WINKOWSKI. We have been working on our requirements. We believe that there is a need to continue to explore the technology, particularly for the CSDs.

We believe that if we are going to have a CSD it has got to meet our standards. We want to make sure that we don't have a lot of false positives where we are chasing down containers. We also feel that it should be used in a selective mode.

Mr. CUELLAR. Are you all asserting that the technology does not exist?

Mr. WINKOWSKI. No, the technology exists. The question becomes the reliability.

Mr. CUELLAR. Okay. Not promoting any particular product—I want to make that clear for the record—but, I mean, there is some technology that already exists that I think has been validated. Why isn't your testing or the Department's testing from the technology that is available out there?

Mr. WINKOWSKI. Well, we understand there is a technology out there, and we also believe that there is application out there. We don't believe that they should be hung on all 11.4 million seaport containers coming into the country, number one. Number two, it should be used on a selective basis; and, number three, we have got to make sure that we are testing that technology. Because if you have a device that is reliable at 95 percent or 96 percent, you are talking about many containers where you could have false positives on. So we are working through those issues. We are not dismissing the use of CSDs.

Mr. CUELLAR. Would you keep the committee advised on your progress on that at least?

Mr. WINKOWSKI. Absolutely. Absolutely.

Mr. CUELLAR. On the transportation worker identification credentials—I guess this is to the Coast Guard—you all sent out a security alert I guess just less than a week ago dealing with Long Beach and L.A. possibility of gang members dock workers, organized criminal elements trying to solicit information on TWIC. Any further status on that?

Captain STURM. Congressman, I don't have anything to add at this time. I would clarify that I think that was an attempt at our local office there to just alert local facility operators that there are criminal elements looking to exploit, you know, gather information for possible exploitation in the future. But there was no indication that there was any success in that area.

Mr. CUELLAR. Okay. All right. Well, thank you.

I have no further questions, Madam Chair. Thank you.

Ms. SANCHEZ. The Chairwoman recognizes the gentleman from New Jersey, Mr. Pascrell, for 5 minutes.

Mr. PASCRELL. Thank you.

I want to thank everyone for their service to their country, but I still believe strongly that port security remains one of the biggest homeland security vulnerabilities in our Nation and more has to be

done and a sense of urgency, I think, has to be part and parcel of our everyday work so that we can face these threats.

The SAFE Port Act was passed by Congress as a strategic plan to enhance the security of all of our ports, but the many agencies within the Department of Homeland Security have fallen too far behind in implementing key provisions.

Last year, we passed the critical legislation I authored with Dave Reichert from Washington, a member of this committee, to direct the Secretary to establish a port securities training program. This program was intended to enhance the capabilities of each of our Nation's seaports to prevent and to prepare for response to and to mitigate against acts of terror, to mitigate against natural disasters and other emergencies by providing validated training to all disciplines that are involved in operations and safety at our ports.

So my question, Captain Sturm, is, has the Coast Guard established port security training and exercise programs which is required by the SAFE Port Act? It is our understanding that port workers still lack the necessary training. Could you be brief and to the point?

Captain STURM. Yes. Mr. Congressman, under MTSA 2002 there were some existing requirements for training and exercises. Model courses for facility workers as well as members on the shipboard community were developed. Now extra money has been allocated to Florida State University which has been developing actual courses that specific unions, employers and other groups can use, more or less off-the-shelf, to build their own training programs, making it that much easier to conduct training.

So we continue to move forward on building—providing assistance for training to people in the maritime community.

Mr. PASCRELL. Thank you.

Are you satisfied with the progress of not only the training but the exercises that were very definitive in the port securities bill?

Captain STURM. Well, with respect to exercises, that process continues to evolve as well. The first 2 years after MTSA 2002, most of our exercises focused on the prevention and protection nature of area maritime security plans. Last year, approximately 35 percent of our exercises also included recovery and reconstitution. This coming year, we expect 50 percent of those exercise will. So, as maritime security efforts mature in ports, our exercise program will continue to mature as well; and we will provide additional guidance to our field units.

Mr. PASCRELL. Assistant Commissioner Winkowski, although it was recommended by the GAO and the SAFE Port Act that minimum technical operating standards for nonintrusive inspection equipment at CSI ports have yet to be established, without such standards, what assurances does our Nation have that this equipment that you have been talking about is capable of detecting weapons of mass destruction within these high-risk containers?

Mr. WINKOWSKI. Well, we rely on the expertise of the scientists from an operations standpoint, whether it is Department of Energy or the DNDO.

Mr. PASCRELL. Where are you with the standards? How can you make an evaluation or a judgment unless you have established the standards by which we can conclude that we are protecting this

Nation from weapons that I have described coming into our ports, and what assurances can you give us if you don't have the standards?

Mr. WINKOWSKI. I don't have the answer to that question.

Mr. PASCRELL. I think that is pretty significant, don't you, that we get the answer?

Mr. WINKOWSKI. Yes, I agree.

Mr. PASCRELL. Because everything is evolving here. The favorite word of Homeland Security is "evolving." Life is evolving. I believe in evolution of ideas, evolution itself, but we have got to get to a point where—we are never going to have a seamless situation. Nobody is saying that. Everybody understands that. But we can be doing much better in terms of the length of time we have had to put this together.

The resources that everybody says we have, Madam Chairwoman, we have these resources. We don't need more money. We do not need this or we don't need that. Then why don't we ever get to the point where we are saying, we are satisfied, we have established a standard, and we have met that standard?

And I would like to ask, if I may, one more question.

Ms. SANCHEZ. I will indulge the gentleman from New Jersey for his question.

Mr. FANGUY. Ms. Fanguy, how do you expect poor operators and trucking companies to continue operating in the face of the provisions that have been laid out in the SAFE Port Act and the TWIC program, in the face of these provisions which may mean a significant chunk of their workforce will now be ineligible to enter the ports in the first place?

Ms. FANGUY. We have established a very robust appeals and waivers redress process for workers. And we certainly understand that some people may have some of the criminal disqualifiers in their past, but we want to work very closely with these workers.

The process that we have laid out is the same as that that we use in the HAZMAT program. And I want to reassure you that we work closely with the drivers in the HAZMAT program today. Based on the most recent statistics that we have, we have processed approximately 700,000 drivers through the HAZMAT program; and in terms of waivers that have been denied, we have denied approximately 70.

So for people who will work with us, we want to make sure that we can get the information to be able to clear their information. If it is an appeal and we have incorrect information, we want to correct that. If it is somebody who has something in their past and they no longer pose a security threat, we will work closely with them to make sure that we can note that and give them the credential that they need.

So we are doing it today on HAZMAT, we will use the same process on TWIC, and we want to reassure you that it is something that is very important to us.

Mr. PASCRELL. Thank you.

Ms. SANCHEZ. Let me get a clarification on that. You said you denied 70 under the HAZMAT?

Ms. FANGUY. That is correct.

Ms. SANCHEZ. How long has the HAZMAT program been going?

Ms. FANGUY. The HAZMAT program has been going approximately 2 years now.

Ms. SANCHEZ. How many HAZMAT certifications have you given out?

Ms. FANGUY. Seven hundred thousand.

Ms. SANCHEZ. Seven hundred thousand. Good. Thank you for that. We wanted that on the record.

I would thank the panel for being before us, and we will again thank you for your work. We will probably have some other questions which we will put in writing to you, and we hope that you will get back the information we need as quickly as possible.

We will dismiss the first panel and ask the second panel to please approach and get ready, and I will give a 5-minute intermission for people to stretch their legs and get business done, and we will be back in 5 minutes with the second panel.

[Recess.]

Ms. SANCHEZ. I welcome the second panel of witnesses.

Our first witness is going to be Mr. Lindsay McLaughlin, the chief lobbyist—that is the first time I have heard you called a lobbyist—chief lobbyist for the International Longshore and Warehouse Union. In this role, since 1991, he has advocated for a wide variety of issues to benefit the members of his union, including the process protections for longshore workers undergoing background checks and adequate port security training.

Our second witness is Mr. Robert Blanchet, Representative for the Port Division of the International Brotherhood of Teamsters. He currently represents the Teamsters Port Division on the west coast, serving the ports of Oakland, Long Beach, Seattle-Tacoma and Portland; and in that capacity he helps represent over 5,500 longshoremen, clerks, truck drivers, tugboat deckhands, tugboat captains, port authority employees, guards and warehousemen who work at our Nation's ports. He has been a member of the Teamsters Union for 39 years. Welcome.

Our third witness is Mr. Chris Koch, President and CEO of World Shipping Council, a trade association representing the international liner shipping industry. The Council's members represent over 93 percent of the international liner industry capacity serving U.S. international commerce. Mr. Koch was hired by the industry to establish this organization in August of 2000.

And our fourth witness is Ms. Mary Alexander, Director of Government Relations at Panasonic Corporation North America. She has been with Panasonic for over 19 years, focusing on international trade, tax, and general corporate affairs issues; and she currently chairs the Joint Industry Group, an ad hoc coalition of Fortune 500 companies, carriers, customs brokers, trade associations, service providers and law firms with a common interest in global commerce.

And our final witness is Mr. Wade Battles, Managing Director for the Port of Houston Authority; and as managing director, a position he has held since 1999, Mr. Battles is the equivalent of the chief operating officer, overseeing all of the port's administrative and operational departments. A long-time maritime professional, he has been an active member of numerous industry associations

and committees, including the American Association of Port Authorities and the National Maritime Security Advisory Committee.

And without objection, the witnesses' full statements will be inserted into the record.

Ms. SANCHEZ. I will now ask my friend, Mr. McLaughlin, to summarize his statement for 5 minutes.

STATEMENT OF LINDSAY MCLAUGHLIN, LEGISLATIVE DIRECTOR, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

Mr. MCLAUGHLIN. Thank you, Chairwoman Sanchez and members of the subcommittee. Thank you for inviting ILWU to testify. As you know, the ILWU represents longshore workers on the west coast of the United States.

There are a number of important provisions of the SAFE Port Act that I would like to talk about. First, port security training and exercises. To date, most of our longshore workers don't know what the evacuation procedures are. There haven't been any live exercises.

Recently, the ILWU officers met with Rear Admiral Bone on the west coast to talk about a wide variety of port security issues, including training; and what we told him is that our major priority is that we have a whole cadre of people who are willing and able to work on recovery efforts in case there is an attack and that we need training for these people that would volunteer in HAZMAT and—somebody has got to move these containers out of the way in the event of an incident. We need to start somewhere. That is somewhere.

On TWIC, the rollout is going to be mid-November. Our membership has some concerns, the loss of privacy involved in submitting to the background check. The fee for the card is a burden for some of the lower-paid workers such as security guards. Many of our members have expressed concerns that they are going to go through this process and pay money when there are no readers in place to read the cards.

But our leadership has asked the union to cooperate with the TSA; and we are in discussions at those ports, Honolulu, Oakland, and Tacoma, to establish mobile units in the halls. That is a good thing.

But it is instructive to look at the experience of the HAZMAT truck drivers in obtaining their security clearance. TSA claims that they processed 700,000 applications, resulting in the disqualification of 5,500 individuals. Ninety-five percent of the disqualified individuals did not respond to the initial letters explaining their rights to appeals and waivers, and we are concerned about that for a number of reasons. We are concerned about people not being able to understand the letters that are going to them, perhaps because of literacy or because English is the second language. And it is imperative that a worker understand his or her rights right up front and that they are able to understand this communication that they get. So it needs to be in different languages, and there needs to be interpreters or people need interpreters.

Another concern of the ILWU is the inaccuracy and incompleteness of the FBI rap sheets that will be used to determine whether

a member has passed a background check. The experience of workers in the hazardous materials certification process demonstrates this problem. TSA has reported that more than 3,000 people were initially found to have failed the criminal background check, even though they had actually had no disqualifying convictions and otherwise met the requirement for issuance of a TWIC. These incorrect initial determinations were caused by rap sheets that were incorrect or incomplete or that failed to distinguish between felonies and misdemeanors.

Now, given the wide scale inaccuracy and incompleteness of the FBI rap sheets, TSA must be required to conduct a further investigation before making an initial determination to deny somebody a TWIC and workers must be allowed to continue doing their jobs until the appeals process is exhausted.

Another concern of ours is on the west coast we have traveling longshoremen. They might be a longshoreman in a small port, and there is no work, so they travel up and down the coast. You might have a longshoreman who needs to take care of a sick family member, so he travels to another area. We are concerned about the compliance date; and the compliance date on the west coast we believe should be the same, given that we have traveling people.

Another point I would like to make, the Federal Government is spending millions of dollars on a system to control access to port facilities for perhaps a million American workers. Yet the Department of Homeland Security is missing a huge, gaping hole, so we are going to have this access control for people going in and out of our gates, yet empty containers go in and out of our gates every day unchecked.

And we have this example in the Port of Ashdod in Israel where people did get in through a container and people died because of it. Longshoremen were blown up because of it.

It makes no sense to us that you are spending millions of dollars to control access to our Nation's ports, yet not even a simple pilot program, as I understand it, is going on; and we need to go much further than that. This is something that they used to do, check containers as they were going into the gates to ensure that they are actually empty and that there are no people or contraband or things in that container that shouldn't be.

And another issue I would like to wrap up is the port security regulations. Right now, they require terminal operators to check seals to ensure that they have not been tampered with as they are going into the facility and upon storage, and this just is not being done. In fact, some of the terminal operators since 9/11 have discontinued this process because of the competitiveness factor, we believe. And there are regulations in place. We have questions as to why, 5 years after the regulations, there is no enforcement.

Finally, we would like to talk a little bit about the preemption issue. I think several unions have brought this up, and it is an important—that they don't need multiple cards. Either we are going to have a uniform card or we are not.

Again, I appreciate you allowing me to testify today behalf of the ILWU.

Ms. SANCHEZ. Thank you for your testimony.
[The statement of Mr. McLaughlin follows:]

PREPARED STATEMENT OF LINDSAY McLAUGHLIN

Thank you Chairwoman Sanchez and Members of the Subcommittee for inviting the International Longshore and Warehouse Union (ILWU) to testify on the status of the Security and Accountability For Every (SAFE) Port Act.

As you know, the ILWU represents longshore workers in the states of Washington, Oregon, California, Hawaii, and Alaska. We have long advocated the development and implementation of practices to limit the risk of terrorism at our work sites and to keep our ports from becoming conduits for unconventional weapons. To that end, it is imperative that the ILWU workforce be utilized as the first line of defense against maritime terrorist activities; law enforcement and other first responders should recognize us as a natural ally.

Within each jurisdiction, key union officers are members of the Area Maritime Security Committee. Our relationship with the Coast Guard has never been better; we applaud that agency for its cooperation and for performing its job admirably—often with limited resources.

There are a number of important provisions of the SAFE Port Act that deserve immediate attention and action from the relevant agencies. First, the SAFE Port Act requires the Department of Homeland Security, in coordination with the Coast Guard, to establish a port security training program to enhance the capability of each facility to prevent, prepare for, respond to, mitigate, and recover from acts of terrorism or natural disasters. Additionally, the Act requires each high-risk facility to conduct live or full scale exercises not less frequently than once every two years.

The Act calls for training involving evacuation procedures in the event of an incident. Most longshore workers have no idea how to orderly evacuate facilities. To date, longshore workers have not been trained, with the exception of union-conducted initiatives. Our employers resist live exercises because it may temporarily disrupt commerce. However, without live exercises, any plan cannot be tested and improved in the event of unforeseen problems. The disruption to commerce in the event of any large-scale incident would certainly be much more significant with an unprepared workforce.

Recently, ILWU officers met with Coast Guard Rear Admiral Bone in San Francisco for a wide-ranging discussion of port security. The ILWU emphasized our high priority placed on training. It is critical for our nation's economy that our members get back to work as soon as is practical and safe following an incident. Someone will have to move containers out of the way; commerce will have to resume. Our union needs to be integrated into the emergency command structures. We have discussed with our employers forming a voluntary cadre of longshore workers to train for and be prepared to work in potentially hazardous environments. While discussions are helpful, we must begin implementation as soon as possible.

The Transportation Security Administration (TSA) began enrolling individuals for a Transportation Worker Identification Credential (TWIC) at the Port of Wilmington, Delaware on October 16. On the West Coast, TWIC will initially be rolled-out at the Ports of Honolulu, Oakland, and Tacoma in mid-November. Workers will be charged \$132.50 for a card lasting 5 years. Our membership has raised many concerns with TWIC, including the loss of privacy involved in submitting to a background check. The fee for the card is a burden for lower paid workers such as security guards. Our members are also concerned that the card will be used for purposes other than simple access control. There is a fear amongst longshoremen that truckers and other individuals who must gain access to the port will not have to be compliant given the industry's fear that there may be a trucker shortage. Longshore workers see this issue as a matter of fairness that every individual on the docks, regardless of occupation—management and labor alike—should have to go through the same process. Finally, it may be years before card readers are installed at our nation's ports. It makes little sense to issue cards to people for the purpose of access control without having readers for the cards.

The ILWU leadership has urged our Locals and ILWU members to cooperate with TSA and Lockheed Martin to enroll our members in an orderly fashion. Discussions are occurring with these entities to establish a mobile unit at the union halls or in the vicinity of the union halls to accommodate our workforce.

It is instructive to look at the experience of Hazardous Material truck drivers obtaining their security clearance pursuant to the USA PATRIOT Act. TSA claims that they processed 700,000 applications resulting in the disqualification of 5,500 individuals. Ninety percent of the disqualified individuals did not respond to the initial letters explaining their rights to appeals and waivers. The ILWU is concerned with this statistic for a number of reasons. We are concerned that thousands of individuals may not have understood the communication to them because of literacy issues or perhaps because English is the individual's second language. It is impera-

tive that a worker be able to understand his or her rights during this process if initially denied a card. This means that TSA must make materials available in multiple languages, not merely English and Spanish, and must make interpreters available to ensure that the non-English-speaking members of our workforce are able to continue their work in the industry. It is equally important that all written materials be drafted using plain language that can be easily understood.

Truck drivers have a choice whether to transport hazardous materials or not; longshore workers do not have a choice. Longshore workers must have a card to work unless an escort procedure is worked out with the terminal and approved by the Department of Homeland Security. Given the importance of this card to our members' livelihoods, we urge the TSA to revise their regulations to allow some initial waivers to be granted to an individual without having to apply for the waiver.

Another concern of the ILWU is the inaccuracy and incompleteness of the FBI "rap sheets" that will be used to determine whether our members pass the background check. The experience of workers in the Hazardous Materials certification process demonstrates this problem. TSA has reported that more than 3,000 people were initially found to have failed the criminal background check even though they actually had no disqualifying convictions and otherwise met the requirements for issuance of a TWIC. These incorrect initial determinations were caused by rap sheets that were inaccurate or incomplete or that failed to distinguish between felonies and misdemeanors. These approximately 3,000 workers were able to successfully utilize the appeals process to correct the erroneous initial determination. However, it is almost certain that an untold number of other workers who were erroneously denied certification did not appeal, perhaps because they did not understand their rights or could not read the information provided to them. Thus, in addition to these 3,000 workers who successfully appealed, there are almost certainly countless others who met the requirements for a Hazardous Materials certification, but are now barred from hauling Hazardous Materials because of inaccurate or incomplete records.

In the ports, where workers will have to have TWICs in order to keep their jobs, the impact of the faulty records has the potential to be far more damaging. Workers who are denied a TWIC will lose their ability to work in the industry altogether. And even those workers who appeal an incorrect initial determination and ultimately prevail will be unable to work until the appeals process is complete. This means that a worker erroneously denied a TWIC, will be off work for at *best* several months while he or she appeals the incorrect determination. Given the wide-scale inaccuracy and incompleteness of the FBI rap sheets, TSA must be required to conduct a further investigation before making an initial determination to deny someone a TWIC and workers must be allowed to continue doing their jobs until the appeals process is exhausted.

We would be very surprised if any members of the ILWU are terrorism security risks. Last year, the Coast Guard asked the union to cooperate in checking our members' names against the Terrorist Watch List; they presumably found no matches. We remain adamant that felony convictions for past crimes are not necessarily an indication of a terrorism security risk. We urge TSA to utilize the waiver procedures included in the Act. The Coast Guard must adequately staff independent Administrative Law Judges to hear appeals from individuals denied a waiver. And as with the appeals process, workers should be permitted to keep their jobs while they are exhausting the waiver process.

At the Senate Commerce Committee hearing on port security on October 4, 2007, Senator Cantwell asked the TSA how they would accommodate longshore workers who travel to work across various port zones. We are concerned that the response from TSA is ambiguous. Each Captain of the Port will determine when their zone is ready for TWIC compliance. The ILWU has an established travel system whereby workers regularly move between ports. Workers at small ports where work is scarce may not yet require a TWIC card but seek work in the ports where the TWIC cards are indeed required. Thus, the compliance date for implementation of TWIC must be uniform on the West Coast.

The federal government is spending millions of dollars on a system to control access to port facilities for perhaps a million American workers. Yet the Department of Homeland Security continues to ignore a gaping hole in the maritime security system. Empty containers are a real risk as a means to transport weapons or people. Few terminals on the West Coast are visually inspecting containers to ensure that they are indeed empty. Given that empty containers are unsealed, it is easy for an individual to climb into a container and gain access to secure areas of a port facility. The SAFE Port Act requires a pilot program that includes the use of visual inspections of empty containers. We are not aware that any pilot program has begun. We recommend that the Committee go much further and simply require that

facilities visually inspect the empty containers, given the expensive investment we are making to control access through the TWIC program.

There have been legitimate concerns raised by our counterpart on the East Coast, the International Longshoremen's Association, and the sea-going maritime unions over states and localities such as Florida implementing their own version of TWIC. Workers should only go through one TWIC process and the due process protections embodied in federal port security law must apply to all states and localities.

On March 14, 2004, ten dock workers were killed in the Israeli Port of Ashdod by suicide bombers; these terrorists were able to enter the port facilities undetected by hiding inside a cargo container. We must not experience a similar tragedy before we get serious about the cargo and empty containers that enter our port by sea or by land.

Existing port security regulations require that container seals be inspected to detect and deter any tampering when entering a port facility and upon storage on the docks. This is simply not being done at most facilities; unbelievably, some facility operators have discontinued this practice since September 11, 2001 in order to further enrich themselves. Is there some reason that these important regulations are not being implemented 5 years after the Maritime Transportation Security Act was signed into law?

The Act requires the National Institute for Occupational Safety and Health and OSHA to evaluate the environmental and safety impacts of non-intrusive imaging technology and to develop and put into place a radiation risk reduction plan to minimize the risks to workers and the public. Such evaluation needs to proceed. We are alarmed at the lack of independent study of the long-term effects of this technology on the human body. The ILWU will continue to place the safety of our members' lives first.

In conclusion, the ILWU urges that port security training and exercises move from discussion to action. Longshore workers should be trained to assist in the recovery efforts in the event of an incident. We urge the Committee to go beyond the pilot program on empty containers and mandate the visual inspection of empties, especially given the focus on access control at our ports. We urge that current regulations requiring seal inspection actually be implemented and enforced. An independent study on the safe use of radiation devices must go forward. Finally, the TWIC implementation must not jeopardize the livelihoods of workers who do not pose a terrorism security risk.

Thank you for this opportunity to testify.

Ms. SANCHEZ. And now we will hear for 5 minutes from Mr. Blanchet to summarize his statement.

STATEMENT OF ROBERT F. BLANCHET, TEAMSTER PORT REPRESENTATIVE, INTERNATIONAL BROTHERHOOD OF TEAMSTERS

Mr. BLANCHET. Chairwoman Sanchez, Ranking Member Souder and members of the subcommittee, my name is Bob Blanchet, Representative of the Teamsters Port Division. I serve on the San Francisco Bay Area Port Commission, where I work with Captain Uribe of the U.S. Coast Guard.

While the TWIC is just now being implemented in the Port of Wilmington, tens of thousands of port truck drivers go unchecked in our Nation's ports every day. Indeed, many port drivers show up and are issued a day pass to circumvent security systems that some ports like Savannah, Georgia, already have in place. The ports look the other way because moving containers trumps security.

Today, security checks for most truck drivers consists of merely flashing a license, a license that could be forged or fraudulent. Let me tell you, that is exactly the case for the port of Oakland. I watch drivers every day being waved into the port terminals by flashing their commercial drivers' licenses to the security guards. The security guard has no way of knowing that the driver he just

let through the gate has a forged CDL, or commercial driver's license.

I am not talking or making up a story. I will take any member of this committee to a truck stop on Santa Ana Boulevard in Oakland, California. That is where a little white van often drives up as a convenient drive-in counterfeit center. You pay \$200 up front and the friendly vendor opens up a side door and pulls out a blue curtain for a backdrop, takes a picture. You return a few hours later and you pay a second \$200 for your almost instant license. It takes place at every port.

Last Friday, I called and asked one of our organizers in Los Angeles to pick up a couple of counterfeit licenses. He got his at the corner of Pacific and Florence in Huntington Park. I have them here, one in the name of Bennie Thompson, one in the name of Michael Chertoff. The fake license business is so competitive in Southern California that they only cost him \$100 each. And I would like to submit the drivers' licenses.

Ms. SANCHEZ. "Class A" meaning?

Mr. BLANCHET. Class A driver's license. I have mine here. Anybody on the committee that would like to look at one. I have a HAZMAT endorsement. I have every endorsement.

Ms. SANCHEZ. That would be the commercial trucker's license.

Mr. BLANCHET. This is a valid, legal driver's license. Those two are fraudulent, forged.

Don't tell us that you have the situation under control. When TWIC is implemented on the west coast, nothing will change until the readers are in place. The mob producing false CDLs, green cards, Social Security cards, and DLT medical certificates will easily produce fake look-alike TWIC cards.

Already, before the TWIC is implemented, there is a whole industry in existence right now where the drivers who have credentials bring containers out of the port and hand them off to other drivers who may not have a port credential, a HAZMAT endorsement or even a CDL. These containers are dropped right on the street outside the port terminal gate and picked up by these drivers.

Similarly, a terrorist without a TWIC can drop a container in the street outside of a port and hand it off to a TWIC credentialed driver and take it inside.

I have photos we took this past weekend that shows our port container relay operations. Every person who drives a container truck or handles or repairs or stores a container inside or outside the port terminal should be required to have a TWIC identification card.

We look forward to working with the committee and finding realistic ways to create a safe port. I look forward to answering any questions that the subcommittee members may have. But also I would like to say this on behalf of my family, my children, and grandchildren: Thank you for your hard work and please save this country in the future for them.

Ms. SANCHEZ. Thank you, Mr. Blanchet. I thank you for your testimony.

[The statement of Mr. Blanchet follows:]

PREPARED STATEMENT OF ROBERT F. BLANCHET

Chairwoman Sanchez, Ranking Member Souder, and Members of the Subcommittee:

My name is Bob Blanchet, Representative for the Port Division of the International Brotherhood of Teamsters. We represent over 5,500 longshoremen, clerks, truck drivers, tugboat deck hands, tow boat captains, port authority employees, guards and warehousemen who work at our nation's ports. I have been a member of the Teamsters Union for 39 years, working in the freight industry as a driver before being elected as Vice President and then President of Local 287 in San Jose, California. I have served as a business agent and organizer as well, and currently represent the Teamsters Port Division on the West Coast—serving the ports of Oakland, LA-Long Beach, Seattle, Tacoma and Portland.

I am in and around the ports on a daily basis and have an opportunity to interact with port drivers and other port workers regularly. I have been appointed to serve on the San Francisco Bay Area Port Security Commission, where I work with Captain Harold Uribe of the Coast Guard. I have witnessed first hand the dedication and concern of this Captain of the Port in implementing security measures to protect our ports against potential terrorist attacks.

It is a daunting task to secure both the land and seaside areas of a port. Are the ports more secure one year after enactment of the SAFE Port Act? Certainly, improvements have been made in some areas, but in others, security is severely lacking. And while the Transportation Worker Identification Credential (TWIC) is a noble effort to control ingress and egress into and out of the ports, the Teamsters Union has many concerns with the structural and planning shortcomings of the TWIC and how this program will work on the ground when finally implemented. These include driver turnover; cost of the TWIC and other forms of ID required by various ports; efforts already underway to circumvent container pickup in the ports; the lack of readers allowing for potential counterfeit TWICs; the possible loss of work while drivers apply for the TWIC and wait out the waiver and appeal process if needed; and the list of disqualifying offenses themselves. We are supposed to be weeding out potential terrorists, not denying jobs to hardworking port workers who may have an irrelevant transgression in their past.

Driver Turnover Presents Security Challenges

As the Teamsters Union pointed out in our earlier testimony before the combined MARAD/Coast Guard field hearings, the assumptions of driver turnover are way out of whack! The port drivers are not a stable workforce like the dockworkers and other port employees. According to statistics provided by the American Trucking Association, these poor exploited drivers have an annual turnover rate of 120% per year. This figure dwarfs the 12% average turnover rate used by TSA to estimate the resources and cost needed to implement the TWIC. Poor and abusive working conditions have created these astronomic turnover rates for short-haul container drivers, which will make it virtually impossible for TSA to collect names, let alone conduct background checks and issue TWICs quick enough to keep commerce flowing efficiently through our ports. The Coast Guard recognized this problem last year, when it failed to include port drivers in its initial Maritime Identification Credentials notice issued on April 28, 2006. And it continues to confirm this difficulty by refusing to implement Section 125 of the Safe Port Act (PL 109-347) that required port drivers to undergo the same security protocol as every other port worker—the check against the terrorist watch list and the immigration status check.

While the TWIC is just now being implemented at the Port of Wilmington, hundreds of thousands of port truck drivers go unchecked in our nation's ports every day. Why is this happening? Unlike longshoremen and other port employees, there is no one in the ports that can account for port drivers. And I have to believe that the ports have not pushed this requirement because they fear an immediate driver shortage. There is no one who can provide names of all the port drivers operating within any given port. Indeed, many port drivers show up and are issued a day pass to circumvent permanent credentialing that some ports already have in place. The ports look the other way because moving containers trumps security.

Under the current system, most port truckers are incorrectly classified as independent contractors. The drivers' status as independent contractors has grave implications for port security. To begin with, because they are considered independent contractors, no one—not the motor carriers or brokers who utilize the drivers, nor the steamship lines nor the shippers—take responsibility for identifying who drivers are or assuring that drivers are properly credentialed. Second, as independent contractors, drivers are at the bottom of the port's economic ladder, typically netting \$11 to \$12 per hour for a working day that often stretches to 12 hours. Drivers are not entitled to statutory benefits, such as worker's compensation and typically do

not have access to medical insurance or retirement programs. Under these conditions, it is not hard to see why the port driver turnover rate is so high.

The Ports of Los Angeles and Long Beach are considering enacting a concession model for port trucking which could solve many security problems related to port trucking. The two ports are considering requiring all motor carriers providing drayage services at both ports to utilize employee drivers to operate newer, environmentally "clean" trucks. The requirement that companies utilize employee drivers means that motor carriers will be responsible for assuring that their drivers are properly screened and qualify for TWIC. The Teamsters applaud the Ports' efforts to improve security and urge the Committee to support this program.

Lack of Card Readers Allow Security Gaps

Today, security checks for most port drivers consist of merely flashing a license—a license that could be forged or fraudulent. Let me tell you—that is exactly the case in the Port of Oakland. There is no main port gate at Oakland. Each terminal has its own entrance. I watch drivers every day being waved into the port/terminal entrance by flashing their Commercial Drivers License (CDL) to the security guard. In most cases, these current forms of identification are not even looked at. If a guard recognizes the driver, he waves the driver onto port property. And, that security guard has no way of knowing that the driver he just let through the gate has a forged CDL.

I am not making up a story. I will take any Member of this Committee to an area near the Port of Oakland. That's where a little white van often appears as a convenient drive-in counterfeit center. You pay \$200 up front and the friendly entrepreneur opens up his side door, pulls out a blue curtain for a backdrop and takes your picture. You return a few hours later, pay a second \$200 and pick up your almost instant license.

I would maintain that when TWIC is implemented in the Port of Oakland, until card readers are installed, nothing will change. Nothing will change because the TWIC will be forged within 48 hours. It won't have a fancy chip or biometric identifier in it, but on its face, it will be good enough to fool the security guard, especially the ones who don't even bother to closely examine it. And it won't present itself as any layer of security if guards continue to wave drivers through without even looking at the credential.

Off-Port Facilities Create Security Gaps

Already, before the TWIC is implemented, there are ways that drivers without proper credentials are circumventing the system. There's a cottage industry in existence now where drivers, who have credentials, bring containers out of the port and hand them off to other drivers who may not have a port credential, a hazmat endorsement, or even a CDL. These containers are dropped right on the street outside the port terminal gate and picked up by these other drivers. The same thing happens when the containers come back to the port. With very few empty containers checked on return, we don't know who has brought that container from where and what he has put in it.

In previous testimony before the Senate Committee on Homeland Security and Government Affairs, the Teamsters Union testified about the issue of containers sitting in the ports for days without being screened for radiation. Radiation detection equipment should be positioned so that containers coming off the ships are screened immediately. In many instances, containers are moved to on-site rail yards and other holding yards and may sit for days before they are screened—and only when they eventually leave the port.

This raises further questions about security as containers move through the entire chain of custody from the port and are returned to the port. While all local port truck drivers who actually perform work inside the port terminal will be background checked to obtain the TWIC, what about those drivers who fail to secure the proper TWIC or who avoid the background checks altogether because of known legal problems or worse. They can continue to take part in the off-port drayage business by either rail, distribution work, or trans-load facility work or by batching boxes with someone who has TWIC credentials and can do the interchange in or out of the port gates.

Every day, hundreds of intermodal boxes turn up missing, loaded with everything from tennis shoes to hazardous material. Sometimes these loads are not missed for days or even longer because of a broken system that invites disaster. What about rail workers, off-port lift operators, cross dock employees, marine chassis, box, or refer maintenance mechanics who have full access to every part of critical intermodal equipment outside the port gates, or intermodal trucking company employees who handle the assignment of container loading and unloading? Also, containers sit on rail sidings for hours and days without any security at all, or on vacant lots, at

shopping malls, or on neighborhood streets or at fuel stops. "Batching" takes place outside along side streets near the port or at rail gates. This practice involves taking care of paper work during normal hours of port operation and then moving loads or empties outside the gate and dropping containers along the street or in unsecured vacant lots for later delivery by others or possibly by the same trucker. This is done to move as many boxes as possible during normal port business hours into or just out of the port gates. It is also used by drivers who don't want to come into the port because of congestion, waiting times, or who may have legal issues keeping them from taking a chance of being checked by security. Some of these drivers have no hazmat credentials stamped on their CDL license to haul this type of material or are possibly driving under revocation or suspension, maybe without insurance, current tags, or maybe even worse.

Here's a perfect example. The Port of Savannah in conjunction with the county & state of Georgia supported a surprise action of checking workers for outstanding warrants. This led to dozens being arrested on child support violations among other issues. However, in a matter of a few days the majority of trucking companies managed to get their boxes into & out of the port by increasing the batching. Other trucking companies, worried about a shortage of drivers, were willing to go into the port to make special arrangements for those drivers who refused to pass their boxes off to a clean local driver. These drivers pick up a container at a rail yard, distribution center, or customer warehouse and bring it not to a port terminal but to an "outside drop location" or container yard. Workers at that off-dock container yard do not undergo background checks or have to obtain the TWIC. For that matter, the managers and owners of those yards are not checked either. A closer examination of off-port storage yards, rail yards, near dock container yards and warehouses is necessary to ensure that security is not compromised in an effort to avoid the TWIC and other security credentialing.

Credentialing Fees Create a Financial Hardship

The Teamsters Union has testified in the past about its concern for port drivers making \$10—12 per hour having to pay \$132.50 for the TWIC. We are also concerned about the lost time truckers may experience in visiting the enrollment center and waiting for their TWIC, especially where waivers or appeals may be involved. If drivers are forced to pay this fee, they should not have to pay additional fees at every port they enter or, as in the Port of Miami, each time a driver switches companies, he must pay for a new credential.

There should be one federal credential—the TWIC. It should allow access to all U.S. terminals, and there should not be an additional terminal ID card issued for each maritime operator with an extra fee for port truck drivers and other maritime workers. The card should follow the worker and not be able to be removed by the employer, the terminal operator, nor the terminal operator's private police force. Only official federal government agencies such as the TSA or the U.S. Coast Guard should have the authority to revoke the TWIC. The port terminal operator should not have the right to discriminate or ban union workers, organizers or any individual on any basis other than being a security threat to the terminal as determined under the TWIC program. To vest authority to revoke the card to employers, port authorities and others, gives extraordinary power to intimidate, harass, and threaten workers into possibly ignoring safety and health rules, work rules and other protections for workers. Imagine having the power to decide unilaterally if a driver can work in a port. Taking away his TWIC denies him his livelihood. That should remain the function of the TSA and the Coast Guard.

The Florida Uniform Access Credential

The Teamsters Union strongly questions the need for the State of Florida's FUPAC—the Florida Uniform Port Access Credential, once the TWIC is implemented. While every port has the right to determine who can enter its facility on official business, each state should not be able to layer additional security requirements on its maritime workers. To do so will defeat the purpose of the TWIC—that is allowing workers to move from port to port, and will essentially create 50 different requirements for entrance to a state's ports. It is our understanding that the State of Florida wants to vet workers who have been granted a waiver under the TWIC, to separately determine their suitability for working in the Florida ports. It is inconceivable that a worker who has been background checked under the TSA protocol and then undergoes further examination by TSA through the waiver process, which in itself is a multi-layer review process, would pose a security threat that the state of Florida must further examine. This is not an acceptable practice and TSA should not enter into any agreement or Memorandum of Understanding with the state of Florida to allow this to move forward.

Disqualifying Offenses

Despite recent actions by Congress to codify disqualifying felony convictions, the Teamsters Union still strongly believes that the list of disqualifying offenses, in several instances, is not indicative of crimes that would make one a terrorist threat. We encourage the TSA to continue to outreach and communicate with potential applicants for the TWIC to make sure that those applicants understand the ability to request a waiver or appeal. More importantly, we encourage the TSA to act judiciously in reviewing waivers and appeals, understanding that they alone may determine the ability of these applicants to continue to make a living and provide for their families. Security is of utmost concern to everyone. No one wants to see another terrorist attack in this country, but we also must be cognizant of the rights and privacies of our citizens.

Security at the ports has improved somewhat as a result of enactment of the SAFE Port Act. But much more needs to be done to address the gaps that still exist. We look forward to working with the Committee to achieve this objective. I look forward to answering any questions the Subcommittee Members may have.

Ms. SANCHEZ. And I now recognize Mr. Koch to summarize his statement for 5 minutes.

STATEMENT OF CHRIS KOCH, PRESIDENT, WORLD SHIPPING COUNCIL

Mr. KOCH. Chairwoman Sanchez, members of the committee, thank you for the opportunity to be here on the oversight hearing on the SAFE Port Act.

As has been discussed here today, the SAFE Port Act is a multifaceted strategy for how to deal with this challenge; and DHS is proceeding hopefully in close coordination with this committee as it develops the various initiatives.

Today, I would like to point out that the Coast Guard is proceeding with the long-range tracking initiative mandated by the SAFE Port Act. It has a proposed rulemaking out allowing comments by the end of the year. We are fully supportive of that initiative.

Much has been said on the TWIC already here today, and many experts are here. I will not spend time on the TWIC. But certainly the objective of the TWIC is to address the very problems Mr. Blanchet just identified, and we are hopeful that it will be able to do that in as expeditious a fashion as possible, recognizing, as DHS is trying to do, they do not want to stumble as they implement it.

I want to spend a minute talking about supply chain security or container security aspects of the SAFE Port Act.

The government strategy right now makes a lot of sense, which is to do 100 percent screening of all containers before vessel loading. What they do is perform stop, and any box they have a serious question on before it is put on a ship for the U.S., when it gets to the U.S., do 100 percent radiation screening of all boxes coming into the U.S. and then 100 percent inspection of any container they have a question about. We think that is a reasoned approach, and we think it is working.

In order to do that, the SAFE Port Act mandated that risk assessment to be improved should get better data, better data to perform this risk assessment. That is the 10 plus 2 initiative that Assistant Commissioner Winkowski spoke about. That MPRN is not yet published. We are hopeful it will be published soon, and from a strategic perspective we think that the CBP is doing exactly the right thing. There will be some controversy in the trade about it

because getting more data is not easy, but we think they are doing exactly the right thing.

As to CSDs which were discussed briefly—several times here today, I would point out that there is no definition or set of proposed requirements for CSD yet at this point. There is no common agreement of what a CSD must be, what it must accomplish. There is no definition yet of what frequency it should operate in, what the requirements should be, what false positives should be, what permissible false negatives would be, what the reading infrastructure would be, how that reading infrastructure would interface with CBP and how it would be acted on. All of those issues will have to be addressed, and DHS is going through them at the present time.

I would point out that the one device that several members put up in the air today is not interoperable with other vendors' devices. So it would make no sense not to have requirements out there that all had the opportunity to comment on and understand, and we hope that what CBP will do is put out a pilot program to test these devices so we can all learn from them.

Finally, I would like to speak on the issue of 100 percent container inspection. As you know, that was not part of the SAFE Port Act, but it was recently added to our statutory framework by H.R. 1 or the implementing 9/11 Commission recommendation act.

We would urge the committee to recognize that what has happened as a result of that provision is that a substantial part of the world, the governments, our trading partners, are confused about what the strategy is of the U.S. Government toward container inspection; and I would hope that this committee, working with DHS, could help try to address those questions of where really are we going on this, who is it that is actually expected to do the container inspection if we are going to go to 100 percent?

There are certainly terminal operators out there who might be willing to invest in it if the government of the United States would recognize them as legitimate people to do it. But it is people like Dubai Ports World who in the past have had issues that the Congress did not regard them as appropriate to do this. So we are asking foreign governments to do it.

Also, the question of what is to be done with the images generated by the equipment that is mandated, that is a huge issue. Recognizing that they are very complicated, recognizing that this mandate is out there, we would encourage the committee to work closely with the Department to try to bring some understanding. Because this is truly an issue that has terminal operators and governments around the world scratching their head trying to figure out exactly what the intention of the U.S. Government is.

We would be happy to work with the committee in trying to answer some of those questions, and I thank you for your time.

Ms. SANCHEZ. Thank you, Mr. Koch.

[The statement of Mr. Koch follows:]

PREPARED STATEMENT OF CHRISTOPHER KOCH

I. Introduction

Good afternoon and thank you for the invitation to testify before the Subcommittee today. My name is Christopher Koch. I am President and CEO of the World Shipping Council (WSC or the Council), a trade association that represents

the international liner shipping industry. I also serve as the Chairman of the National Maritime Security Advisory Committee (NMSAC), a Federal Advisory Committee Act committee providing advice to the Coast Guard and the Department of Homeland Security (DHS) on maritime security issues, and as a member of the Commercial Operations Advisory Committee (COAC) that advises the Departments of the Treasury and Homeland Security on commercial and Customs matters.

Liner shipping is the sector of the maritime shipping industry that offers service based on fixed schedules and itineraries. The World Shipping Council's liner shipping member companies provide an extensive, network of services that connect American businesses and households to the rest of the world. WSC member lines carry roughly 95% of America's containerized international cargo.¹

Approximately 1,000 ocean-going liner vessels, mostly containerships, make more than 22,000 U.S. port calls each year. More than 50,000 container loads of imports and exports are handled at U.S. ports each day, providing American importers and exporters with efficient transportation services to and from roughly 175 countries. Today, U.S. commerce is served by more than 125 weekly container services, an increase of over 60% since 1999.

In addition to containerships, liner shipping offers services operated by roll-on/roll-off or "ro-ro" vessels that are especially designed to handle a wide variety of vehicles, including everything from passenger cars to construction equipment. In 2006, these ro-ro ships brought almost four million passenger vehicles and light trucks valued at \$83.6 billion into the U.S. and transported nearly one million of these units valued at \$18 billion to U.S. trading partners in other countries.

Liner shipping is the heart of a global transportation system that connects American companies and consumers with the world. More than 70 percent of the \$700 billion in U.S. ocean-borne commerce is transported via liner shipping companies.

The international liner shipping industry has been determined by the Department of Homeland Security to be one of the elements of the nation's "critical infrastructure".

Liner shipping generates more than one million American jobs and \$38 billion in annual wages. This combined with other industry expenditures in the U.S. results in an industry contribution to U.S. GDP that exceeds \$100 billion per year.

II. The Focus on Maritime Security

For the past six years, the WSC and its member companies have strongly supported the various efforts of the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to enhance maritime and cargo security. The multi-faceted and risk-based strategies and programs of the government have been able to make substantial progress toward meeting this challenge, and they continue to evolve.

At the same time, the Coast Guard and CBP recognize the fact that the industry is transporting on average roughly 50,000 containers, holding roughly \$1.3 billion worth of cargo owned by U.S. importers and exporters, each day through U.S. ports. Significant delays to this flow of legitimate commerce could have substantial adverse effects on the American economy.

The multi-layered maritime security strategy has a number of parts on which I will briefly comment today. The basic architecture of U.S. maritime security is well known and understandable. First, there is vessel and port security, overseen by the Coast Guard and guided in large measure by the International Ship and Port Facility Security Code (ISPS). Second, there is personnel security, overseen by various Department of Homeland Security agencies and the State Department. Third, is cargo security, which with regard to containerized cargo, is addressed through Customs and Border Protection's advance cargo screening initiative, C-TPAT, and the Container Security Initiative—all of which are reinforced and made more effective by the increased deployment of container inspection technology at U.S. and foreign ports.

A. Vessel and Port Security Plans

Every commercial vessel arriving at a U.S. port and every port facility needs to have an approved security plan overseen by the Coast Guard. Each arriving vessel must provide the Coast Guard with an advance notice of arrival 96 hours prior to arriving at a U.S. port, including a list of all crew members aboard—each of whom must have a U.S. visa in order to get off the ship in a U.S. port.

The liner shipping industry's operations are consistent and repetitive—its vessel services and crews call at the same ports every week. So long as there is consistent and professional implementation of the security rules, which is usually a hallmark

¹A listing of the Council's member companies and additional information about the Council can be found at www.worldshipping.org.

of the Coast Guard, liner shipping has found no problem in operating in the new vessel or port security environment.

We also appreciate the Coast Guard Commandant's admonition that the "concept of maritime security cannot be reduced to a single threat vector". There are numerous potential vectors for terrorists attack on the maritime environment that don't involve cargo containers. For example, merchant vessels are in fact defenseless against small boat attacks. We fully support the Coast Guard in its efforts to secure an enormous Maritime Domain against a variety of risks.

Long Range Information and Tracking (LRIT) of Vessels: On October 3, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) on Long Range Information and Tracking (LRIT) in the Federal Register. The Council supports the LRIT objective and the enhanced visibility of vessels offshore that it will give to the Coast Guard and other governments.

The Coast Guard expects existing maritime satellite communications equipment to be able to meet these tracking requirements. Assuming this is correct, the Council does not foresee major problems complying with these regulations.

The LRIT system is based on a network of data centers sharing information. A vessel will transmit its data to the data center selected by its flag administration. This data center could be a national center, like in the U.S., a regional or cooperative center, perhaps like the European Union, or an international center, open to any country to join. Coordinating the sharing of information between the data centers is an International LRIT Data Exchange (IDE). The IDE is the body that is connected to all other LRIT data centers and routes information between LRIT data centers. The IDE shares information in accordance with the LRIT Data Distribution Plan.

There may be concern, however, regarding how the Coast Guard intends to implement LRIT if the International Data Center (IDC) is not in place. The IDC is where a vessel whose country of registration has not established its own data center is to send its position reports. Many smaller nations were expected to use the IDC and how their vessels will comply with the LRIT requirements is in question. An agreement has been reached to allow the Coast Guard to host the International Data Exchange (IDE) on an interim basis until January 1, 2010. It is unclear what happens with the IDE after that date. A uniform, global operating system is the desired objective. The Coast Guard has invited comments on these issues in its recent NPRM, and we expect that the industry and other governments will be considering these issues closely.

Small Vessels: The attacks on the *U.S.S. Cole* and *M/V Lindbergh* demonstrated that large vessels can be the objects of terrorist attack from small boats. The U.S. Coast Guard Commandant, Admiral Allen, has on numerous occasions noted this and other small boat vulnerabilities and the difficulty in devising effective ways to address the threat without significantly inconveniencing recreational and small boat movements. The Council notes that DHS has recently undertaken some pilot efforts on the West Coast to test technologies that may contribute to addressing this issue, and while we recognize the difficulty of the challenge, we believe that such DHS effort are focusing on a legitimate concern. We also appreciate that the U.S. Coast Guard is playing a lead role in having put this on the International Maritime Organization's agenda in order to develop international principles and criteria for addressing this issue.

B. Transport Worker Identification Credential

The Council supports the credentialing of maritime workers requiring unescorted access to secure maritime facilities. The National Maritime Security Advisory Committee (NMSAC), with the advice and input of a wide range of U.S. maritime interests, has spent considerable effort to provide comments to the Coast Guard and the Transportation Security Administration on the development of the TWIC regime. The industry's primary concern is that the security enhancement envisioned in this new system not have undue impacts on those personnel who work in port terminals servicing vessels or on port operations.

The SAFE Port Act requires TWIC reader pilot projects to be run in at least five locations. NMSAC has recommended that the final TWIC regulations should not be published until the results of these pilot projects are known.

The Coast Guard has indicated its intention to issue two sets of proposed rules on the TWIC regulations: the initial set to give some shape to the pilots and the second, supplemental proposal which is intended to finalize the proposed regulations when the pilots' results are known. We support this measured approach.

The Coast Guard also recently announced the biometric standard to be placed on the TWIC card. This standard contains two items that were not supported by the industry: encryption and a Personal Identification Number (PIN). The industry's

concern has been that encryption will create operational complexities which have the potential to severely impede the flow of maritime commerce. Further, the NMSAC does not believe the significant additional costs associated with encrypting the fingerprint template are warranted given the minimal risk involved without such encryption. How these two items will work with readers remains to be seen, but the industry is hopeful that the good consultative process that the Coast Guard has established with NMSAC will allow for these issues to be addressed satisfactorily.

Lastly, DHS has begun to enroll workers in Wilmington, Delaware, and has also listed the next eleven follow-on locations for enrollment. The industry strongly supports a measured implementation of this challenging new regime so that any unanticipated issues that may arise can be addressed as the system is rolled out in stages.

C. Containerized Cargo Security

The WSC fully supports the U.S. government's strategy in addressing containerized cargo security. Specifically, the Council supports CBP's risk assessment and screening of 100% of all containers prior to their being loaded onto vessels destined for the U.S., and the pre-vessel loading inspection of 100% of those containers that CBP's cargo risk assessment system determines to present a significant security risk or question.

The Council does not support recent legislation's call for inspection of 100% of all import containers before vessel loading, because the concept has not been clearly considered and remains presently impractical.

1. Container Security Initiative (CSI)

The network of bilateral Customs-to-Customs agreements forming the "Container Security Initiative" (CSI) continues to grow. There are now 58 foreign ports participating with the U.S. in this initiative, covering 85% of U.S. containerized import trade. CSI is a keystone to the effective international implementation of the advanced screening and inspection of U.S. containerized cargo that presents security questions. It is only through these cooperative CSI Customs-to-Customs data sharing and container inspection cooperative efforts that overseas container inspection can occur.

The United States' approach to supply chain security up until now has been dominated by an interest in inbound or imported cargo. This is understandable, but as supply chain security regimes become more globalized, and as our trading partners call for "reciprocity" and "mutual recognition" of security improvements, it is very important that the Department of Homeland Security plan for and implement a coordinated strategy for dealing with the nation's international import and export maritime commerce.

When CBP calls for a foreign Customs authority's assistance to check a container it has a question about before vessel loading, so must it plan and be able to act on that same foreign Customs' authorities request for assistance on checking a U.S. export container that may raise a question. When discussing with foreign governments "mutual recognition" of supply chain security protection programs, the U.S. government will be called on to address what programs enhance the security confidence of U.S. exports to the same extent that other governments' programs enhance the security confidence of their exports. We believe that Customs and Border Protection is the right agency for establishing and ensuring a consistent and coordinated U.S. approach to such issues, and that additional planning should be undertaken in this regard.

It is for this reason that the Council recently wrote to CBP to recommend that the agency plan for how to expand its CSI Customs-to-Customs cooperative partnerships with European customs authorities to prepare for the planned 2009 implementation of the European 24 Hour Rule under Commission Regulation 1875. The purpose of such planning would be to ensure that American export commerce receives the same kind of cooperative and expedited consideration when European authorities raise security questions, as European export containers receive today when CBP raises such a question.

We also note that, five years after Congress passed the supply chain security amendments to the Trade Act, disagreement between the U.S. Departments of Homeland Security and Commerce still prevent regulations from being issued to implement Section 343(b) of that Act (19 U.S.C. 2071(b)), which calls for rules regarding the advance documentation of U.S. export waterborne commerce.

2. Containerized Cargo Screening and Risk Assessment

CBP employs a multi-faceted containerized cargo risk assessment and screening system, so that it can identify those cargo shipments that warrant further review,

rather than those that are low risk and should be allowed to be transported without delay.

C-TPAT: One element of that system is the Customs' Trade Partnership Against Terrorism (C-TPAT) pursuant to which various entities in the supply chain voluntarily undertake security enhancing measures. CBP then validates participants' compliance, and compliant supply chains are accordingly afforded lower risk assessments.

24 Hour Rule: Another important element of the risk assessment system is CBP's receipt and analysis of pertinent advance information about cargo shipments before vessel loading. This program began soon after September 11th, under which carriers provide CBP with the advance shipment information they possess 24 hours before vessel loading in a foreign port for risk screening (the "24 Hour Rule"). The Council has fully supported this regulation and this strategy, which allows the CSI program to perform advance container risk assessment.

Better Security Screening Data: "10 plus 2" Initiative: While the 24 Hour Rule has been in the Council's view a logical and sound effort, the Council has for several years noted that more effective advance cargo security screening will require more data than the information provided by carriers via the 24 Hour Rule.

Recognizing both this need for enhanced container security targeting and the existing limits of information provided in carriers' bills of lading, the SAFE Port Act sets forth the following requirement to enhance the capability of CBP's Automated Targeting System:

"Section 203(b): Requirement. The Secretary, acting through the Commissioner, shall require the electronic transmission to the Department of *additional data elements for improved high-risk targeting, including appropriate elements of entry data*. . .to be provided as advanced information with respect to cargo destined for importation into the United States *prior to loading of such cargo on vessels at foreign ports.*"

Customs and Border Protection (CBP) is developing a regulatory proposal that would require U.S. importers or cargo owners to file ten additional data elements² with CBP 24 hours prior to vessel loading, and to require ocean carriers to provide two additional sources of data—vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This is referred to as the "10 plus 2" initiative.

CBP has undertaken extensive, transparent, and open consultation with the trade and carrier community in developing this proposal. It is our understanding that the proposed regulation to implement this new requirement should be published in the Federal Register for public comment in the near future, with implementation beginning sometime in 2008.

While the private sector obviously needs to await the actual proposed regulation before providing comments in the expected rulemaking, we would note that CBP's efforts in developing this initiative have been transparent, professional and cooperative, and are in pursuit of a strategic objective that is not only mandated by the SAFE Port Act, but is highly logical in order to enhance containerized cargo risk screening.

Global Trade Exchange (GTX): Other pending efforts within DHS regarding the acquisition of additional cargo shipment information for enhanced risk screening are less understood by the trade. Notwithstanding the fact that CBP has not yet published, let alone implemented, its proposed "10 plus 2" regulations requiring additional information for cargo risk assessment, DHS officials have indicated that the Department will be proceeding with efforts to commence an additional trade data gathering and analysis effort under the name of the "Global Trade Exchange" or GTX. This initiative has not yet been clearly explained to the industry.

What we understand at the present time is that DHS is considering awarding funding for an initial phase of this initiative. It is our understanding that participation by members of the trade providing such additional data is expected to be voluntary, that the party to collect the data would be drawn from a restricted number of commercial entities acting as a third party data clearinghouse, and that secure and confidential treatment of any data provided is recognized to be needed.

What services, analysis or risk assessment competence would be required of such vendors is unclear. What the specific data to be gathered would be has not been explained. The extent to which such shipment data would be shared with other gov-

²The ten cargo data elements of the new Security Filing have been identified by CBP as: (1) Manufacturer (or Supplier) Name and Address, (2) Seller (or Owner) Name and Address, (3) Buyer (or Owner) Name and Address, (4) Ship To Name and Address, (5) Container Stuffing Location(s), (6) Consolidator (or Stuffer) Name and Address, (7) Importer of Record Number, (8) Consignee Number, (9) Country of Origin, and (10) Commodity 6-Digit HTS Code.

ernments is not clear. How this system would be integrated into CBP's existing Automated Targeting System is unclear. How such a commercial third party data manager would make money off this program is unclear, and who would bear what costs for participating in such a system is unclear. What the uses of the data, other than assisting Customs with supply chain risk assessment, would be are unclear. How the data in the system would be protected is unclear. Whether ocean carriers would be expected or invited to participate in the provision of information is unclear. What benefit would result from participating in such an effort is unclear.

DHS has indicated that the intent is to proceed under a "request for quotation" solicitation process, which is restricted to a limited number of vendors now established in the DHS "EAGLE" procurement program.

In short, the GTX effort has not yet been explained by the government and is not yet understood by the trade. U.S. importers with whom the Council has discussed this initiative are confused by this process. There is some concern within the trade community over the apparent development of such an initiative without the government's usual transparency and process of consultation. COAC has written to the Secretary of DHS requesting consultation on this initiative.

3. Container Inspection

DHS has a well established strategy to undertake radiation scanning of all containers entering the U.S. before they leave a U.S. port. CBP recently deployed its 1000th container radiation portal monitor as it gets closer to its objective of performing radiation scanning on 100% of all inbound containers at U.S. ports of discharge.

CBP also undertakes non-intrusive inspection technology (NII) or physical inspection of 100% of all arriving containers that are determined to pose a significant security question. CBP has no plans and no capability, however, to inspect every arriving container. Because that is not practical, the agency is utilizing, and soon will be enhancing, its cargo risk assessment system and the CSI program to identify which containers do warrant inspection.

In order to further consider the issues involved in the application of additional container inspection at overseas ports of loading, DHS has undertaken the "Secure Freight Initiative", under which pilot projects are being established at several foreign ports testing more complete pre-vessel loading scanning, generating possible lessons to be learned for broader application of pre-vessel loading container inspection efforts.³

The "Implementing the 9/11 Commission Recommendations Act", which was signed into law in August, includes the well known provision requiring that by 2012 100% of the containers imported into the United States be "scanned" before being loaded aboard vessels destined for the United States, meaning that the container would have to be run through radiation detection equipment *and* non-intrusive imaging equipment before vessel loading. What, if anything, would be done with the images or data produced by those scanings was not addressed by the law, nor were a host of other highly relevant questions, including who was to perform this task, and whether the U.S. would perform such scanning of its own export containerized cargo. The WSC issued a six page statement on this legislation on July 30th, which is available on the Council's website.

Many foreign governments are obviously and justifiably concerned about the implications and meaning of this new U.S. law. We expect that they will continue to inform the U.S. government of their concerns, including their view that this statutory provision expects foreign governments to undertake measures for their exports that the U.S. government has no intention to undertake for its exports.

The shipping industry's customers—the hundreds of thousands of U.S. importers and exporters who use containers to transport their cargo—are also concerned about the meaning and potential effects of this law. The port terminal operators around the world that service the industry's vessels are also concerned but unsure about the intent or effect of this statute.

Several things seem clear. First, implementation of this law's stated objective would require addressing many serious issues that the statute does not address, including the fact that implementation of overseas container inspection requires the cooperation of foreign governments. Second, the U.S. government has no current plans to scan 100% of its outbound export cargo containers, and thus foreign governments' predictable inquiries about reciprocity will likely be unanswerable. And, if

³DHS has established three full scale container scanning pilots in co-operation with host governments at Southampton, U.K.; Puerto Cortes, Honduras and Port Qasim, Pakistan. Three other smaller scale pilots are under development at port facilities in Busan, South Korea (Gamman Terminal); Salalah, Oman, and Singapore.

the United States' trading partners do not implement 100% container scanning, there is nothing that the U.S. government can realistically do about it other than cease trading with the rest of the world. We therefore see the obvious need for further international dialogue on this matter.

At this time, this provision of the "9/11 Commission Recommendations Act" is an indecipherable riddle. The world has no idea what to make of it and does not know if it expresses the real strategy of the United States or not.

If the Congress intends to pursue any kind of meaningful dialogue or progress on determining what would need to be addressed in order to pursue this statute's stated vision of 100% container screening at foreign ports, then we respectfully submit that it should begin to consider and address a number of critical questions, including the following:

1. *Whom Does the Law Intend To Perform the Container Scanning?* The legislation pointedly fails to address the issue of who is to perform this activity. It does not require U.S. Customs to do this, as it is clearly impossible for the Congress to require U.S. Customs to undertake such activities within the jurisdiction of other sovereign nations. It does not require foreign governments to do so, as it has no such authority. The legislation simply says that containers shall be scanned. By whom? Who is to purchase, operate and maintain the equipment?

Is this a sovereign function to be handled by governments? Is this a private sector function? Before private marine terminal operators could seriously consider such an investment and activity, the Congress would need to provide clarity on this point and who would be trusted to perform the task and under what circumstances.

Does Congress intend that non-government foreign port facility operators would perform this task? The 109th Congress took the position that one of the largest port facility operators in the world, Dubai Ports World, was an unacceptable security risk to buy a U.S. marine terminal operating company and hire U.S. workers, working under U.S. management, to service vessels in U.S. ports. Would Congress consider that company acceptable to perform this task in foreign ports? The largest terminal operating company in the world, Hutchison Whampoa, is owned and controlled by the Chinese. Would Congress consider that company acceptable to perform this task?

Even if the Congress were to determine that such terminal operating companies were appropriate entities to install and operate the necessary scanning equipment, and even if these companies were willing to make the capital investments necessary to install and operate this equipment, the law fails to answer who will review, interpret and analyze the readings produced by the technology. It is extremely unlikely that these terminal operating companies would accept the responsibility or the liability for the actual analysis and assessment of the scanning technology.

2. *Failure to Define the Scanning Requirement:* Recognizing that 100% container "inspection" is impractical, the statute requires instead that every container be "scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel." This by itself would be pointless.

The law fails to address whether the scanning data actually has to be reviewed and analyzed, and if so, under what circumstance, when and by whom? The law fails to address whether or when the data from the scanning equipment is transmitted to the U.S. government and at whose cost. There are many complexities and costs involved in addressing these issues.

Is every container radiation scan to be reviewed before vessel loading, with mandatory secondary inspection if there is an unusual radiation reading?

Is every NII scan to be reviewed before vessel loading? Or, is it only those containers that trigger a certain threshold in CBP's Automated Targeting System that require review of NII scans? If only a few percent of the containers would have their NII images reviewed before vessel loading, what is the point of requiring 100% of all containers to have NII images? Why not just perform NII inspections on the containers that present security questions?

3. *No Reciprocity:* The statute purports to require 600 ports around the world to approve, implement, and utilize such technology, systems and processes for all cargo destined for the U.S. or effectively face an embargo on their exports, when the U.S. government does try or plan to perform this function on its export cargo, and scans virtually no U.S. export containers. If implementation of this law were actually pursued, it is entirely possible, if not highly likely, that foreign governments would establish "mirror image" requirements on the U.S.,

forcing all American export containers to undergo radiation and NII scanning before vessel loading at U.S. ports—requirements which the U.S. government and U.S. port facility operators are presently and for the foreseeable future incapable of meeting. Is the Congress prepared to fund such a system for U.S. exports?

4. *Threshold Technology Question:* The statute provides that DHS may “extend” or waive the scanning requirement, if: “(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.” NII container inspection technology does not have any government or commercially accepted software that enables “automatic notification of questionable or high-risk cargo”, putting aside the relevant question of defining what would constitute “questionable or high-risk cargo” that the technology would need to identify. Does this mean that until NII equipment can meet such a standard that has yet to be defined and agreed upon, that this statutory mandate is not applicable?

The “9/11 Commission Recommendations Act” provisions calling for 100% overseas container scanning has raised more questions than it has answered.

4. Seals and Container Security Devices

The SAFE Port Act included the following directive: “Not later than 90 days after the date of enactment of this Act, the Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States.” (Section 204(a)) It was not evident what this provision meant or how it might be interpreted, and the section’s time deadlines were not going to be met.

Accordingly, the “9/11 Commission Recommendations Act”, Congress amended this section by providing that: “(B) Interim Requirement.—If the interim final rule described. . . is not issued by April 1, 2008, then. . . effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers. . . .” Thus by next October, all U.S. inbound containers will be required at a minimum to have ISO standard security seals. This provides helpful clarity.

As to the government’s view of “container security devices” (CSDs), things are less clear. First, CSD is not a defined term. For example, some say that a seal is a CSD; some say a seal is not a CSD. The Council has understood that DHS was planning to issue proposed draft technical requirements for container security devices and the operating protocols associated with such devices by the end of this year for public review and comment. We understand that the DHS Science and Technology Directorate prepared a draft of such requirements that is undergoing further review and amendment within the Department.

The Council and other members of the trade have requested that CBP/DHS allow for full transparency into the development of this effort and solicit public comments on the draft requirements, after they have completed internal government review.

There are at present many unanswered questions about CSD requirements, including what specifically the device would be required to do and its security value, what acceptable false positive and false negative reading rates would be, what radio frequency would be used, the requirements for the installation and operation of the necessary device reader infrastructure, the requirements applicable to the necessary communications interface and protocols with CBP, the security vulnerabilities of such devices, the necessity of interoperability of various vendors’ devices and systems, the data to be captured and transmitted by the device, identification of who will have access to the data in the device, survivability and vulnerability of the device, power or battery life requirements, the probability that the device can be detected or removed without detection, required data messaging formats, event logs, and data encryption.

These questions are even more complicated in the environment of international maritime commerce than they would be in a more controlled environment of U.S. border stations where CSD reading infrastructure would be under the sole control of CBP.

The Council believes it is essential, if an interest in CSDs is to be pursued, for the government to undertake a fully transparent and very clear articulation of its draft views on the requirements for such technology and the related operating systems and protocols, and to provide the public with a meaningful opportunity to comment upon such draft requirements, *before* they are advanced as an element of the government’s container security strategy.

III. Conclusion

Vigilance against terrorist risks requires the development and implementation of prudent security measures, and the continuing enhancement of such measures as the risks change and take new forms. The international trading system is too valuable and important to be left unattended.

The liner shipping industry fully understands this and has cooperated with national governments and international organizations trying to construct meaningful security regimes. The industry will always be concerned that these measures not unduly delay or restrict commerce or impose costs that produce little added security; however, it has supported and will continue to support measures that are well designed and provide real security value with as little impact as possible on legitimate trade.

This is clearly difficult work, but there are clearly some success stories. The International Maritime Organization's development of the International Ship and Port Facility Security (ISPS) Code, the Proliferation Security Initiative, the Container Security Initiative, the "24 Hour Rule" advance cargo screening strategy and its imminent enhancement, the C-TPAT program—all have enhanced supply chain and maritime security. The government's expanded use of container inspection technologies is another example of sound strategy and implementation.

If we are to continue to make progress in enhancing maritime and supply chain security, progress is more likely to occur if:

1. There is a clear and specific definition and agreement on what should be done to improve security.
2. There is a clear and thoughtful prioritization of initiatives.
3. There is sufficient certainty and clarity in purpose to do it right. In the absence of that, time and resources are poorly used and the efforts are less likely to improve security.

We appreciate the Subcommittee's continued interest and oversight of these issues, and would be pleased to provide additional information that may be of assistance to the government in addressing these issues. Thank you again for the opportunity to testify.

Ms. SANCHEZ. And I will now recognize Ms. Alexander to summarize her statement for 5 minutes.

STATEMENT OF MARY ALEXANDER, CHAIR, JOINT INDUSTRY GROUP

Ms. ALEXANDER. Madam Chairlady, Mr. Souder and other members of the subcommittee, my name is Mary Alexander, Chair of the Joint Industry Group, a coalition of trade community members engaged in global commerce. I also am representing my own company, Panasonic of North America, headquartered in New Jersey, with sales, research and manufacturing in 24 states and the third largest U.S. electronics importer, bringing in over 20,000 containers per year. I will comment on the views of JIG members regarding government programs that provide security to our Nation's ports and affect businesses, their supply chains, and their efforts to provide products to the consumer safely, quickly and at affordable prices.

To remain competitive, U.S. companies face pressures from customers to deliver products fast and affordably. Shipping a container of products to numerous consignees is complicated. Any disruption to the supply chain can affect the efficient business process, increasing costs and wait times for retailers and consumers. Therefore, as the Federal Government proposes new security programs, consultation with the business community is critical.

JIG strongly supports the multi-layered, risk-based approach to supply chain security developed by DHS and strengthened by Congress with the SAFE Port Act and other initiatives. These programs will strengthen our Nation's security, once properly implemented.

Just as the need to strengthen border security is critical, so is the need to safeguard the smooth flow of legitimate international commerce. As more security programs are created, the business community faces increased burdens in their operations that can add debilitating costs and delay to business approximate. JIG therefore urges Congress and the administration to remain engaged in dialogue with industry on security initiatives to develop programs that are truly effective and minimize disruptions to the supply chain.

Four specific comments: C-TPAT represents the core of CDP's cargo security program, a government and private sector partnership. This voluntary program has more than 7,500 participants, including Panasonic. While membership levels continue to climb, real benefits remain elusive. Land border crossings have fast lanes, but tangible benefits for ocean cargo, such as reduced inspections, are not apparent and hard to verify. While the investment in C-TPAT membership is real and substantial, members increasingly feel that the promised returns have not been materialized.

The introduction of 100 percent scanning at several foreign ports is an excellent opportunity to assess the viability of the secure freight initiative. We are pleased that Congress in its oversight role will have an opportunity to review a report from CBP due in April on the results of this pilot project. We encourage to you review these results before considering widespread implementation of the program.

The trade community has spent considerable time working with CBP on its 10 plus 2 initiative. Unfortunately, nearly a year after it was presented, we are still waiting for the proposed rules for the initiative. We understand that rulemaking process takes time, but we are concerned that the trade community will have sufficient time to comment and implement the MPRM after its release.

This past August, JIG raised several concerns with DHS about the proposed global trade exchange, including questions on security, confidentiality and cost. Until we have enough information, JIG neither supports nor opposes this program. CBP has been responsive to the trade community in developing other trade security initiatives, but so far development of the GTX appears to be behind closed doors.

JIG appreciates the openness and availability of CBP and DHS staff to consult with the trade on the roughly 30 Homeland Security programs to which businesses are asked to comply. However, the lack of real information on proposed new programs, growing concern that increased costs far outweigh promised benefits, emerging skepticism that the programs are necessary to protect our country, and compliance concerns from our trading partners all need more serious consideration.

Congress' help in getting responses from the administration through public hearings like today's is greatly appreciated. Madam Chairwoman, on behalf of JIG, thank you for this opportunity to testify. I will be happy to answer any questions.

Ms. SANCHEZ. Thank you, Ms. Alexander. I would like to thank you for your testimony.

[The statement of Ms. Alexander follows:]

PREPARED STATEMENT OF MARY ALEXANDER

Introduction

Madame Chairwoman Sanchez, Ranking Member Souder and other members of the subcommittee, thank you for the opportunity to testify on the one-year anniversary and implementation of the SAFE Port Act. My name is Mary Alexander, and I serve as the chair of the Joint Industry Group (JIG). JIG is a broad coalition of Fortune 500 importers and exporters, shippers and carriers, customs brokers and forwarders, trade associations, service providers, and law firms with a common interest in global commerce. In fact, a number of our members including Hewlett Packard, Intel and Panasonic Avionics are headquartered in California.

JIG frequently engages Congress and the Administration on a variety of international trade-related issues, often focusing on issues involving port and border security and customs. In particular, we work closely with U.S. Customs and Border Protection (CBP), the Department of Homeland Security (DHS), the Department of Commerce (DOC), USTR, and Congress to promote international trade policies that reflect the needs of both government and the private sector to secure the supply chain while facilitating legitimate commerce.

While I am here to articulate JIG positions, I also am here to represent my own company, Panasonic Corporation of North America, headquartered in Secaucus, NJ and employing more than 6,000 workers in the U.S. The company sells consumer electronics, industrial products and professional equipment to the American consumer and is the American subsidiary of Matsushita Electric Industrial, headquartered in Osaka, Japan. Panasonic North America is the third largest electronics importer, bringing more than 20,000 containers into the U.S. annually. While worldwide the company has over 300 factories, Panasonic ships products from Matsushita factories in nine countries, with nearly 90 percent of imports coming from ports in Singapore, China, Malaysia, and Japan and to Seattle/Tacoma or LA/Long Beach on the west coast.

In my testimony today, I will provide the views of JIG members regarding the implementation of government programs to provide needed security to our nation's seaports one year after the enactment of the SAFE Port Act. I will also offer real life examples of how government policies affect businesses like Panasonic, their supply chains, and their efforts to provide products to the consumer safely, quickly and at affordable prices.

In order to remain competitive in today's global economy, Panasonic and other U.S. businesses face constantly increasing pressure from our customers to deliver high-quality products faster and more affordably. Unfortunately, shipping a container of multiple products to numerous consignees is a complicated business, and any disruption to the supply chain can adversely impact the efficient business process. For example, Panasonic's supply chain cycle for the Blu-ray disc player is now only six weeks, from the time the order is placed and transmitted to the factory in Japan, to the time the players arrive at the Best Buy distribution centers. This includes an ocean transit time of two weeks and an inland transit time to our distribution center of nine days. Our Lumix cameras, which are shipped by air, have only a four-week supply chain. The timeliness of these supply chains remains critical to the success of our company. Any delays create hardship for our company and increase costs and wait times for retailers and consumers. It is imperative to the viability of Panasonic and other U.S. businesses to guarantee the smooth flow of products for delivery to our customers.

JIG strongly supports the multi-layered risk based approach to supply chain security that has been developed by DHS and strengthened by Congress through the SAFE Port Act and other initiatives. The programs that have been enacted will strengthen our nation's security once they are properly implemented. JIG is concerned, however, that just as the need to strengthen border security is critical, so is the need to safeguard the smooth flow of legitimate international commerce. As more security-focused programs are created, the business community faces increasing burdens in their operations that can add debilitating costs and delays to doing business.

JIG therefore urges Congress and DHS to remain engaged in dialogue with industry on security initiatives in order to develop programs that are truly effective and minimize disruptions to the supply chain. JIG also urges the U.S. Government to propose incentives for companies to encourage participation in these costly and extensive new security regimes.

These issues come to light through JIG's comments on the programs created or affected under the SAFE Port Act noted below:

Customs-Trade Partnership against Terrorism (C-TPAT)

C-TPAT represents the core of CBP's cargo security program. This is a true government and private sector partnership program, based on industry self-policing and self-assessment with verification by government. In sheer numbers, this voluntary program is working well, as evidenced by the more than 7,500 participants, including Panasonic, which was one of the first to join the program. Participants, who attest to the integrity of their security practices and communicate their security guidelines to their vendors and business partners, have been promised a number of benefits, including fewer inspections on their shipments and speedier processing through customs. Real strides have been made on both the certification and validation/revalidation front.

While the membership numbers of C-TPAT continue to climb, the benefits being offered to participants continue to be more elusive. Presently, one real benefit at land-border crossings is evident through the use of FAST lanes, but tangible benefits for ocean cargo, such as reduced inspections, are not readily apparent and are hard to verify. While the investment in C-TPAT membership is real and substantial, members of the trade community increasingly feel as though they made these investments for promises that have not been fulfilled. Even today, five years after the program's inception, C-TPAT participants continue to seek solid benefits in order to justify the numerous costs they incur as a result of the program.

CBP has recently published a C-TPAT Cost—Benefit Survey (Executive Summary included as Appendix A). Based on the reported results, less than one-third of the respondents replied that the benefits of C-TPAT equaled or exceeded the costs from the program. These numbers argue for more tangible benefits. Benefits cannot be just about score reductions, especially as trade and security requirements converge. Suggested new trade compliance benefits, particularly for C-TPAT Tier II and Tier III partners, could include:

- An annual security fee off-set refund based on the number of import shipments and/or
- An expanded use of account-based principles within the C-TPAT program, such as an option for Tier II & Tier III participants to pre-file account-based commercial data in the aggregate.

Finally, in a global economy, programs similar to C-TPAT need to be adopted and recognized among all countries, such as proposed in the World Customs Organization SAFE Framework. A central component of the Framework is mutual recognition among countries, and, in the near term, mutual recognition between the USA and significant trading partners is the key to the success of the SAFE Framework and C-TPAT. Without this, the benefit of remaining in C-TPAT is substantially reduced. We strongly encourage CBP and DHS to continue working with our trading partners to ensure that mutual recognition is accorded to those programs implemented under the SAFE Framework.

Secure Freight Initiative

The introduction of a 100 percent scanning pilot program at isolated locations within several foreign ports serves as an excellent opportunity to assess the viability of implementing the Secure Freight Initiative program unilaterally. Such testing at these ports should be completed before rolling out the program to other ports. This would help to address the biggest concern to JIG members, which is the possibility of delays in inspection and processing containers if the technology has not been sufficiently tested before being implemented. We recommend that Congress, in its oversight role, carefully review the report from DHS, due to this committee in April, on the results of the pilot program. JIG continues to believe that the DHS should implement a pilot program to test scanning technology and only deploy such technology more broadly when it is proven effective and practicable. In addition, Congress should be aware that some of our trading partners have expressed concern about the imposition of requirements such as 100 percent scanning of cargo exported to the U.S.

Advanced Trade Data ("10+2") Initiative

The trade community has spent considerable time working with CBP on developing the requirements for the additional data elements required under Section 203 of the SAFE Port Act to improve CBP's Automated Targeting System (ATS). While the trade was pleased to work with CBP on these requirements, we remain concerned about compliance issues, which could result in an extra two or three days of inventory to meet the reporting requirements. In addition, businesses continue to wait to make any adjustments or rewriting of their own data collection systems until DHS puts out the Notice of Proposed Rulemaking (NPRM) and completes an economic analysis.

Industry has provided input into the development of the NPRM through a "strawman" proposal that was released at the November 2006 CBP Trade Sympo-

sium. In addition, the trade continued to provide input through the Trade Support Network and the COAC. The NPRM will provide an additional opportunity for input from the trade and certainly will clarify the many questions and concerns already raised. Unfortunately, nearly a year later, we still are waiting for the release of the NPRM. In addition, a JIG letter of February 5, 2007 requested CBP, when it publishes its NPRM, to give the trade community sufficient time to prepare for the changes. At a COAC meeting in August, the trade community was assured it would be released soon. It is now the end of October and the NPRM still has not been released. We understand it takes time for rulemaking to make its way through the government, but we urge that this NPRM be expedited and released as quickly as possible.

Per the SAFE Port Act, we also understand that CBP is required to complete a cost/benefit analysis and feasibility study in connection with any additional advance trade data initiative. We are not aware that this report has been completed or has been discussed with the trade. It is important that this report be completed and shared with the trade as soon as possible, as the feasibility and value of "10+2" should be demonstrated before implementing this costly initiative.

It is frustrating that almost a year later we still have no guidance on how this program will be implemented or even what the phase-in period will be. I would like to underscore that the trade community wants to "do the right thing" regarding the intent of "10+2." However, unlike the advanced manifest requirements which merely drew from pre-existing data, the "10+2" initiative will require shippers to develop a brand new process. Panasonic's logistics company says it cannot even begin to re-design its own customs and logistics management system and make other IT changes, let alone alert the factories of additional demands that will be put on them, until it has seen the proposed regulations. All current processes must be reviewed and analyzed to determine how best to have this information supplied from overseas and how to transmit the information. Reprogramming of IT systems can be a long and difficult process and complete information needs to be given at least a year and a half in advance to make sure everything is tested properly. So we need information. We urge the Subcommittee to help move the NPRM process along.

Global Trade Exchange (GTX)

In August of this year, JIG sent a letter to DHS Deputy Secretary Michael Jackson that raised several concerns about the proposed Global Trade Exchange. We understand that DHS envisions this program as the third leg of the Secure Freight Initiative, along with CSI and the "10+2" initiative. JIG circulated this letter widely within DHS and to a number of other government departments. Since then, we have met with government representatives seeking more information, but JIG still has not received any further clarification on the program.

Our questions and concerns remain largely unchanged and include:

- What is the incentive to participate, especially when companies traditionally are extremely reluctant to share confidential information with outside parties?
- What will be the cost of providing data to the exchange?
- How will security and confidentiality concerns be addressed regarding access by third parties and foreign entities?
- What is the added security value beyond what is accomplished by other ongoing and proposed security enhancement programs?
- Will redundant programs such as advance security filings be eliminated?

JIG has neither supported nor opposed this program to date, and that is simply because we have never received enough information to develop a position one way or the other. CBP has been responsive to the trade community throughout most of the development of its various trade security initiatives. As a result of these discussions, numerous adjustments have been made to the proposed programs. This is exactly the manner in which the trade community seeks to work with Congress and the government. Unfortunately, however, development of the GTX has thus far taken place behind closed doors. The trade community has been offered little or no real information, and this is creating widespread concern within our membership.

Container Security Devices

Much of the focus on improving maritime container security has centered on technology in the form of electronic container security devices (CSDs). Considerable improvement in these devices has taken place since emphasis was placed on their development in the post 9/11 trade environment. JIG supports the continued development and voluntary use of CSDs, although we believe the current state of this technology does not yet warrant widespread use.

General acceptance by the trade community will not be achieved until CSDs demonstrate improved performance in several key areas:

Effectiveness: CSDs must be able to consistently detect container breaches and communicate this data to responsible agencies in a timely fashion.

Reliability: The single greatest hurdle CSD technology must overcome is false alarms. Former CBP Commissioner Robert C. Bonner suggested a minimum one percent false alarm standard for electronic container security devices. Even assuming such a standard is achievable, universal usage would hold the potential for false alarms in excess of 100,000 annually. Excessive false alarm rates will undermine confidence in CSDs and lead to costly delays to resolve anomalies. Compliance with minimum false alarm standards must be certified through independent testing by government approved laboratories.

Cost: CSDs must be affordable in order to be commercially viable. Costs range from a few dollars for a simple RFID device to hundreds and even thousands of dollars for sophisticated devices with multiple sensors and GPS, cellular and satellite communications capabilities. Expensive devices add to the cost of business and are thus a competitive disincentive. Incentives need to exist for industry to incur this expense, over the current use of cheaper but still ISO-approved bolt seals.

Response Protocols: Technology aside, there remains a significant need to develop standardized response protocols on how alarms are managed and responded to. Currently, when a CSD registers a container breach, who receives the data generated by the device, and even more importantly, who is responsible for resolving the alarm? Is it CBP, the port authority, the terminal operator, the carrier, the shipper, or the importer? If the CSD alarms overseas, is it the foreign customs administration that must respond? Such procedures are not yet in place for breach alarms generated by CSDs. Since there is no agreement as to who is responsible for resolving container breach alerts, such data now typically goes only to the shipper or the consignee. This may be useful for theft and pilferage analysis, but has no value for national security purposes.

International Customs Treatment of CSDs: The customs agencies of numerous countries have attempted to assess duties and tariffs on devices as they enter or leave the national customs territory. CSDs must be treated as instruments of international trade in language similar to that provided in the UN Convention on Containers. Appropriate HTS classifications must be established through the World Customs Organization and duty-free treatment assured by the World Trade Organization.

To summarize, electronic container security devices hold potential for enhancing the security of our maritime supply chains. To realize this potential, however, much work remains to increase their effectiveness and reliability, provide them at an affordable cost, and develop standardized response protocols to deal with the alarms they generate.

Conclusion

Since 9/11, several government programs have been developed to lower supply chain security risk, including C-TPAT, CSI, Secure Freight, etc. Roughly 30 homeland security programs in the U.S. have been identified to which businesses are asked to comply. JIG members need assurance from federal agencies and Congress that the numerous security-related programs already in place, especially the older programs, are necessary, not duplicative, and remain essential to protecting our country from terrorism.

JIG and its members appreciate the openness and availability of CBP and DHS staff to consult with the trade on efforts to secure our nation's seaports. We are fully supportive of the DHS mandate. However, the lack of real information on proposed new federal security programs, the growing concern that increased costs far outweigh promised benefits from participating in these security programs, the growing skepticism that the panoply of supply chain security programs are all necessary, the added program costs and delays that affect the bottom line of American companies, and the concerns expressed by our trading partners, all need to be more seriously considered. Given these issues, the help of Congress to seek answers to these questions, through public hearings like today's, is greatly appreciated. Madame Chairwoman, on behalf of JIG, thank you for your help and support, and thank you again for the opportunity to present our comments to this subcommittee. I will be happy to answer any questions from you or anyone else on the subcommittee.

Ms. SANCHEZ. I now recognize Mr. Battles to summarize his statement for 5 minutes.

STATEMENT OF WADE BATTLES, MANAGING DIRECTOR, PORT OF HOUSTON AUTHORITY

Mr. BATTLES. Chairwoman Sanchez and the honorable members of the subcommittee, I am Wade Battles, the Managing Director for the Port of Houston Authority. On behalf of the port authority and U.S. seaports in general, thank you for this opportunity to address the subcommittee on important port security matters, including my thoughts on the 1-year anniversary of the SAFE Port Act.

Mr. BATTLES. As you have heard today, the TWIC program faces some daunting challenges and hurdles that must be crossed in a very short period of time.

The Port of Houston Authority supports the concept of a national identification system with background checks for transportation workers and has closely monitored the development of this program. We have had numerous meetings with the Coast Guard and with TSA officials on how we can best facilitate the rollout and the implementation of the TWIC program in our ports.

Our concern is that TSA and their contractor continues to greatly underestimate the number of TWIC cards that will be required and consequently have not allocated sufficient resources in facilities or personnel to efficiently and effectively issue the TWIC card within the timeline mandated by SAFE Port. For example, the whole Houston Port area will have only one permanent facility and four mobile centers. Implementation will start in Houston next month, but critical issues still exist, such as what will be the required credentials, where to pick up completed TWIC cards, payment processes, and other similar issues.

Our other main TWIC concern has to do with the readers. We implore that the readers be fully tested in actual maritime environments, as required by SAFE Port, before any specifications are mandated.

Next, I would like to briefly discuss the 100 percent container scanning provision. First, the Port of Houston Authority joins other U.S. ports in supporting the Federal Government's layered security approach and urges adequate resources be provided to Federal agencies to continue to carry out and improve their security programs. The CSI policy of pushing our borders overseas to inspect cargo before it is actually loaded on U.S. bound vessels has worked well for U.S. ports.

The SAFE Port Act requires DHS to start pilot programs looking at scanning all containers in four selected foreign ports to more fully evaluate the effectiveness and practicality of 100 percent scanning. There is great concern that if U.S. ports require foreign ports to perform 100 percent scanning of all containers destined for the United States, foreign governments could require the same from U.S. ports due to reciprocity. This would have a huge impact on Houston due to a large volume of export cargo that is equal to or greater than our imports. The Port Authority does not have the space nor does CBP have the personnel to scan all export containers. I would encourage this committee to review the findings of the pilot projects and carefully study full ramifications before requiring 100 percent scanning in foreign ports.

Congress has assisted ports with the funding of important security infrastructure. To date, the Port of Houston Authority has

been awarded \$38.6 million in port security grant program funds and urban area security initiative fundings. I would like to compliment DHS on their new structure of the latest supplemental round of funding. By pushing the funding down to the area maritime security committees, the people closest to the port are deciding the priorities for port security. This is an improvement and one that I believe will benefit port security.

I have several other recommendations.

First of all, ports are struggling with the cost for maintenance and operation of the security projects. It would be improper to expect the Federal Government to pick up all M&O costs for the life of the project, but some maintenance and operational costs should be included in the grant application.

Second, the port security grant program should fund the replacement and upgrade of security infrastructure that is already in place. Additionally, the program should allow for upgrading of previously funded security infrastructure as new technology is introduced to maximize the security at our ports.

Before I move on from port security grants, I would like to express our gratitude to this committee for authorizing \$400 million per year in port security grants for the coming fiscal years through 2011 in the SAFE Port Act. DHS has been a good partner with the Port of Houston, and we look forward to working with Congress and DHS to make changes in the program that will improve the overall security of our ports.

In conclusion, I appreciate the opportunity to express my thoughts in SAFE Port at its 1-year anniversary. We believe that this was a good piece of legislation that can be improved with a few adjustments. We in the port industry are dedicated to continue to work with Congress in identifying and providing practical solutions for port security issues.

Thank you very much. I would be happy to answer any questions you might have.

Ms. SANCHEZ. Thank you, Mr. Battles.
[The statement of Mr. Battles follows:]

PREPARED STATEMENT OF WADE BATTLES

Introduction

Madam Chairwoman Sanchez and the Honorable Members of the Subcommittee:
Thank you for this opportunity to address the U.S. House of Representatives Committee on

Homeland Security, Subcommittee on Border, Maritime and Global Counterterrorism.

I am Wade Battles, Managing Director of the Port of Houston Authority.

I am pleased to present my thoughts on the one-year anniversary of the SAFE Ports Act.

Port of Houston

The Port of Houston is a collection of public and private terminals along more than 25 miles of the 53-mile-long Houston Ship Channel. The Port of Houston is the largest foreign tonnage port in the nation, second largest in total tonnage and 10th largest tonnage port in the world.

Most of its cargo is petrochemicals, with more than 150 private refineries, chemical plants and related terminals lining the Port of Houston, the port is home to the world's second largest petrochemical complex.

The Port of Houston, as a whole, is the catalyst for 785,000 statewide jobs, generating more than \$39 billion in personal income annually. Many Texans and other Americans owe their livelihoods to activity tied to the Port of Houston. In addition to jobs, the Port of Houston annually contributes to more than \$117 billion of state-

wide economic value. As you can see from these numbers, the Port of Houston is a large piston of the nation's economic engine.

Port of Houston Authority

The Port of Houston Authority is the local sponsor of the Houston Ship Channel and owns the public terminals of the Port of Houston. The port authority is an independent political subdivision of the State of Texas and is governed by a seven-member board appointed by local entities in Harris County. While the private sector terminals along the channel primarily handle oil, chemicals and other bulk materials; the port authority primarily handles commodities like steel and grain, project cargo, including oil exploration equipment, and its biggest growth area—containers.

The Port of Houston has a long history with containers. In 1956, the first container ship departed New Jersey and arrived in Houston to deliver 58 containers that were secured topside on a retrofitted tanker ship, the *IDEAL X*. In 1977, the port authority opened the Fentress Bracewell Barbour's Cut Container Terminal. The terminal was designed to handle approximately one million twenty-foot equivalent units or TEUs. Barbour's Cut handled 1.6 million TEUs last year. The Port of Houston now handles more than 73 percent of the container cargo market in the U.S. Gulf of Mexico. To keep up with the demand for container capacity, the port authority opened its Bayport Container Terminal in February this year. The Bayport Terminal is designed to handle 2.3 million TEUs at buildout.

An interesting indicator of container capacity demand at our port: in February 2007, we opened the first phase of our Bayport facility, devoting exclusive service to one of our largest customers. We expected the move to relieve some of the pressure from an overburdened Barbour's Cut terminal. However, demand is such that Barbour's Cut Terminal is on pace to break last year's record for container volume.

In 2008, we will open the first of up to three cruise terminals at Bayport. The port authority was the first gulf port outside of Florida to experiment with homeport cruising. Now, several ports have followed suit after witnessing the success of our Barbour's Cut cruise terminal.

Comments

There is no greater responsibility to the Port of Houston Authority than the safety and security of its employees, its visitors and its neighbors. I would like to briefly address the Subcommittee today on the following topics:

1. General comments on SAFE Port Act
2. Comments pertaining specifically to TWIC
3. Port Security Grant Program and suggested modifications
4. The innovative Ship Channel Security District
5. 100 percent Scanning in Foreign Ports and the impact of reciprocity
6. C-TPAT, CSI and other aspects of the security of the international supply chain and
7. CBP Staffing

General comments on the SAFE Port Act

The SAFE Port Act of 2006 is Congress' strongest effort to secure our nation's ports. Among many provisions under the Act, we commend the attention given to improving the ability of the maritime community to respond to transportation security incidents. Particularly helpful are the requirements for area maritime security committees to include business continuity plans as part of their overall plan and the required development of protocols for post-incident resumption of trade.

The Port of Houston is familiar with resumption of trade protocols stemming from near-miss hurricanes, major storm events and fog. The Coast Guard, port authority private facilities and maritime sector along the channel have learned how to cooperatively prioritize vessel movements through practice. It is vital that ports reopen following an incident in an organized and methodical manner.

One of the strengths of the Port of Houston is its close working relationship with the local Coast Guard and Customs and Border Patrol as well as with all other agencies, federal, state and local, that have a role in security.

There is an old saying in maritime circles that says: "When you've seen one port, you've seen one port."

There is a great deal of truth in this, and it is important that our leaders in here in Washington, D.C., who work hard to secure our maritime commerce, both law-makers and regulators, recognize that each port is unique. The best security follows from the ability of local authorities, such as the Coast Guard Captain of the Port, to work with the port members in their district and tailor security requirements to the unique needs and configurations of each local port. Certainly, there must be national security standards, but they must not unduly tie the hands of local authorities, who have the greatest knowledge of unique local conditions and know how to

best secure against their vulnerabilities without unduly impacting critical operational efficiency.

As an example of cooperation at our port, we have been working with local customs officials for several years now to install radiation portal monitors at each of our container facilities. As a result of this cooperation, the port authority is presently in full compliance with regulations requiring that all incoming containers be scanned for radiation by December 31, 2007.

The port authority has signed an agreement with our Coast Guard district, under which we are able to monitor the security cameras of the other in many areas of the Houston Ship Channel and our terminals. Additionally, we have similar camera network-sharing agreements with the City of Houston, Harris County and the Texas Department of Transportation. And, thanks to the substantial help of the Port Security Grant Program, we have a state-of-the-art Emergency Command Center at the Port of Houston Authority, in which we have access to the camera feeds from these regional government bodies. These sharing agreements, along with the emergency command centers that have been constructed in the region are now being linked by sophisticated communication systems that allow each center to be a backup for each other will assist in making the Interagency Operational Center required under the Act truly functional.

We are also working with the United States Coast Guard to amend our Facility Security Plan for one of our primary port terminals to make certain the appropriate areas are covered by the TWIC while minimizing the impact on day-to-day operations but not jeopardize port security. This is an important example, I think, of how Congress and participating agencies all recognize the importance of providing the right balance between security and operating efficiency.

I should mention that there has been concern that Facility Security Officers, Port Police Chiefs and others who take the lead in port security have found that the goal of information-sharing is often impeded by the inability to obtain necessary security clearances, particularly on the federal level, and I would ask the Committee to take up this important issue with the Department of Homeland Security and its maritime-related agencies so that those responsible for port security are not prevented from carrying out their job because they are the last to know of important threat and other security information. We have spoken with a number of ports on this matter, and although there may have been some attempts to address this issue, the concern still remains.

Transportation Worker Identification Credential (TWIC)

A major provision of the SAFE Port Act addresses the Transportation Worker Identification Credential program, commonly called "TWIC." The Port of Houston Authority generally supports the concept of a national identification system with background checks for transportation workers and has closely monitored development of this program. In fact, I am a member of NMSAC—the National Maritime Security Advisory Council—that has studied and advised on many of the issues relating to TWIC. We have a multi-disciplinary security committee at the Port of Houston Authority that has kept abreast of developments in the TWIC program as well as all laws and regulations governing security at our facilities. We have had numerous meetings with Coast Guard officials on how we can best facilitate the roll-out and implementation of the TWIC program at our port.

The TWIC program must be implemented without substantial impacts to the operations of the port. We are now working with our Captain of the Port to re-define our secure areas. Our ports have been historically created with many areas functionally and geographically separate from the cargo loading and unloading along the ship channel. The regulations wisely provide an opportunity to place these areas outside the "secure areas" of our port facilities that will require presentation of a TWIC for unescorted access. We anticipate that we will come to agreement on this issue in a manner that will allow important public non-operational functions to continue outside of the secured areas subject to TWIC compliance.

Last spring, we met with representatives of the Transportation Security Administration and its contractors on the TWIC program. We were surprised that the representatives dramatically underestimated the number of transportation workers at the Port of Houston who would require a TWIC card. Their initial estimate called for 30,000 TWIC cards to be issued in the Houston area. The port authority reviewed the TWIC needs for the Port of Houston with the West Gulf Maritime Association, the East Harris County Manufacturers Association and other groups. The study concluded that we will have approximately 350,000 potential TWIC users in the Houston area.

This information was given to the TSA, which has responsibility for enrollment in the TWIC program. However, we have not seen evidence that TSA has moved

very far off of its original estimate. Nor have we seen substantial efforts yet by the TSA to notify and educate port stakeholders about TWIC.

The port authority was recently informed that TSA would only have a single permanent enrollment center for the Houston area and just four mobile centers. We were also advised by TSA that they are pushing for enrollment sufficient to allow Coast Guard to set September 25, 2008, as the enforcement commencement date. Although we certainly will continue to actively cooperate and do our part in this process, we are concerned that TSA has substantially underestimated the number of TWIC applicants who need to be enrolled in the program in order to achieve timely compliance and while keeping our ports operating efficiently.

Recently, the Department of Homeland Security selected the Port of Houston to be part of the continued rollout for the TWIC next month, November 2007. The port authority is ready to assist the TSA in setting up mobile enrollment centers and otherwise assist the TWIC enrollment process. Our main objective is to improve security through the TWIC process without substantially interfering with efficient operations at our port facilities.

Some modifications to the program that I would suggest are:

- First and foremost that our stakeholders—truck drivers, contractors, stevedores, tenants and others—all get adequate and timely notice of this program and a convenient enrollment center to go to in order to apply for a TWIC and an efficient method to receive their TWIC.
- The TSA should bring the TWIC cards, when ready, to the same mobile enrollment centers that applicants enrolled at or allow the applicant to designate the “pick-up” center in the applicant’s region, rather than forcing the applicants to go to a distant and different enrollment center to pick up their cards.
- The TSA and its contractors need to clarify the identification credentials to be accepted for TWIC enrollment. I believe a driver’s license and a port-issued ID or another second form of government issued identification should be sufficient since that is identification that is reasonable and that a port employee would possess. If a TWIC applicant does not have a passport, requiring an original birth certificate will cause significant problems. The cost and time for obtaining these forms of ID may severely hamper the timeliness and success of the TWIC enrollment program.
- The TSA needs to ensure timely delivery of TWIC cards to new employees. The maritime industry cannot have long delays in credentialing a new port worker. The TSA should work to limit the time it takes to issue a card.

Port Security Grant Program and suggested improvements

Congress has assisted ports with the funding of important security infrastructure since 9–11. The Port of Houston Authority has been successful seeking these funds based on the economic and energy significance of the port. To date, the Port of Houston Authority has been awarded \$38.6 million in Port Security Grant Program funds and Urban Area Security Initiative funding.

I would like to compliment the Department of Homeland Security on the new structure of the latest supplemental round of funding. By pushing the funding down to the Area Maritime Security Committees, the people closest to the port are deciding the priorities of port security. This is an improvement and one that I believe will benefit port security. The Houston AMSC is using the funding to first update its area security assessment. This will give us an opportunity to reevaluate our progress in port security six years after the 9–11 attacks.

Remaining funds will be allocated to projects based on the results of the area security assessment. This is a more regional approach than prior port security grants that were given directly to MTSA-regulated facilities based on criteria established in DC.

Even with the compliments, I do have several recommendations for improving the Port Security Grant Program:

First, the Port Security Grant Program should fund replacement of and upgrades to security infrastructure. As an example, CCTV cameras have about a five—to seven-year life span in the maritime environment. These cameras will need to be replaced. The PSGP does not allow for replacement funding of security infrastructure.

Additionally, the PSGP should allow for upgrading of previously funded security infrastructure as new technology is introduced to maximize the security at ports. This common sense provision will keep port security technology on the cutting edge to prevent and deter possible attacks.

Second, ports are struggling with the costs of maintenance and operation of many of these security projects. However, it would be unfair to ask the federal government to pick up all M&O costs for the life of the project. I believe that if the projects are

rolled into a port's budget, it can adjust its cash flow and other priorities to accommodate the new budget item.

Some of the maintenance and operations costs should be included in grant applications for the PSGP. Currently, the only M&O costs allowed in the PSGP grants are the first year, including during construction/implementation. There is limited need for M&O before the project is completed. I would suggest a 5-year M&O program with a declining percentage each year funded by the grant. For instance:

- Year One, the Grant would cover 100 percent of the M&O costs
- Year Two, the Grant would cover 80 percent of the M&O costs
- Year Three, the Grant would cover 60 percent of the M&O costs, etc.
- After the 5th year of the grant, the port would pick up all M&O costs.

I believe this would allow ports to fund more projects while determining the budgetary impacts of the M&O costs and adjusting accordingly.

Thirdly, under present grant procedures (e.g. Round 7A of the Port Security Grant Program that was announced in a press release on May 10, 2007), a port is given a maximum of three years in which to complete a grant project. That three-year period started on June 1, 2007 for the Port Authority and ends May 31, 2010.

However, even though ports had to submit a budget and the scope with their grant applications last spring, the grant administrators in Washington, D.C. have not given approval to these budgets, and a port cannot commit to a contractor to go ahead with the project until the port receives Washington's approval of this information without risking reimbursement of the funds. In essence, the clock is ticking on our port grants, but we are unable to start on them until we get final approval. It is anticipated that the effect of this is that ports will only have approximately a two-year window (rather than three years as intended) in which to complete their projects because of the inability of the grant administrators in Washington to cut through this review process and approve information that they have now had for some seven months.

I would recommend that the DHS trust its review of the budget and scope at the time of the award and not duplicate efforts by reviewing the same information again.

Before I move on from Port Security Grants, I would like to express our gratitude to Congress for authorizing \$400 million per year in port security grants for the coming fiscal years through 2011 in the SAFE Port Act. This is the funding level supported by the American Association of Port Authorities and its ports.

While I may have a few suggestions for improving the Port Security Grant Program, I must state that DHS has been a good partner with the Port of Houston. We look forward to working with

Congress and the DHS to make changes in the program that will improve the overall safety and security of ports.

Ship Channel Security District

Several years ago, in a series of meetings with the Department of Homeland Security arranged with assistance of Congressman Gene Green, DHS officials detailed the need for a regional approach to security to reduce security risks along the Houston Ship Channel. From those meetings, a new public-private group was created that included Harris County, the Port of Houston Authority, the cities along the Channel as well as the private petrochemical, chemical and refinery facilities along the Houston Ship Channel, including members of the East Harris County Manufacturers' Association.

The public-private group, called the Port Strategic Security Council (PSSC), recognized that the best security for the region would be achieved by a system-wide, layered security approach along with the employment of modern technology and techniques of each individual facility. The PSSC, working with experts in port security, developed a list of projects, regional in focus, to systematically improve security along the Houston Ship Channel. Harris County has sponsored the PSSC's Homeland Security Department Port Security Grants utilizing \$31 million in federal grants for PSSC projects to increase maritime domain awareness, improve interoperability, provide patrol boats and reduce the risk of a terror attack.

The PSSC soon recognized that a mechanism was needed to allow the county, the private facilities, the port authority and others to equitably pay for the local share of the grants and the operation and maintenance of these new security projects. The public-private partners of the PSSC decided the best method to collect these funds could be modeled after assessments collected by state-created municipal management districts.

This year, the Texas Legislature authorized the creation of the Ship Channel Security District. The Department of Homeland Security showed an interest in the legislation as it moved through the process. U.S. Department of Homeland Security

Secretary Michael Chertoff even sent a letter to the Texas Legislature generally supporting the concept of the security district.

The district will be a public-private partnership with the board primarily made up of representatives from private industry. This board will determine the amount and methodology to assess the facilities along the Houston Ship Channel.

Let me point out that the private companies along the channel, and you would recognize their names if I listed some of them, supported legislation that would assess their businesses to pay for improved security infrastructure for the Houston Ship Channel. Instead of waiting for the government to do it, they have stepped up as good corporate citizens to meet the challenge head on. This is another in a long series of examples where federal, state, and local governments, the port authority and the private sector have come together to benefit the Port of Houston.

We have several more hurdles to clear before the district is created. Those include getting more than half of the companies in the proposed district and property owners of more than half the appraised property value of facilities in the proposed district to sign a petition asking for Harris County to create the district.

Once established, this district could be the public-private model for port security nationwide. I would invite the Subcommittee to visit Houston to see first-hand Houston's cooperative spirit in action.

Requiring 100% Container Scanning at Overseas Ports

I would like to briefly discuss the 100 percent container scanning provision in the SAFE Port Act.

First, the Port of Houston Authority joins many other U.S. ports in supporting the federal government's layered security approach and urges adequate resources be provided for federal agencies to continue to carry out and improve their security programs.

The layered, risk-based screening, scanning and inspection policy of cargo containers and the "pushing of the border overseas" to inspect cargo before it is loaded onto U.S.-bound ships has worked well for U.S. ports as well as our foreign partners.

The SAFE Port Act requires the DHS to start a pilot program to scan all containers in four selected foreign ports to more fully evaluate the effectiveness and practicality of this new technology.

I strongly believe that pilot ports are important and the information gleaned from them should be used to help craft any new system. Quick implementation of 100 percent scanning, without incorporating the lessons from the pilot projects, could be both costly and play havoc with our maritime transportation system.

Reciprocity in Scanning

This would be especially true for the Port of Houston Authority, which is one of the few U.S. container ports with balanced import and export container trade. Our strong manufacturing sector in Houston, especially in the petrochemical and machinery sectors, provides us the opportunity to ship many American-made products worldwide. There is great concern that if the US requires foreign ports to perform 100 % scanning of all containers destined for the US, foreign governments could require the same from U.S. ports through reciprocity. The Port authority does not have the space nor does CBP have the personnel to scan all export containers from the Port of Houston Authority.

I would encourage this committee to review the findings of the pilot projects and study carefully the full ramifications of 100 percent scanning in foreign ports.

C-TPAT, CSI and other aspects of the security of the International Supply Chain

The Department's existing programs, many of which were codified in the SAFE Port Act, have been models for enhancing the security of the international supply chain. In 2006, prior to passage of the Act, the Port of Houston Authority signed an Agreement with U.S. Customs and Border Patrol to become a partner with CBP in the Customs Trade—Partners Against Terrorism (CT-PAT) program.

Another successful program codified in the SAFE Port Act is the Container Security Initiative. This program identifies containers that pose a security risk before they are loaded in foreign ports. The port authority supports this program as it provides a voluntary, incentive-based layer of security and enhancement to our port security here in the United States.

Customs and Border Protection Staffing

The Port of Houston and the Houston Airport System had a significant issue a few years ago where the two entities had to share CBP officers. In the morning, the officers were at the port inspecting cargo, but in the afternoons, they were at the airports assisting in processing passengers coming from foreign countries.

This was not an acceptable use of manpower for either the airport or the seaport. Congress rightly came to the rescue by adding new positions for CBP officers over the next six years. Texas Senator Kay Bailey Hutchison even added another 275 CBP officers to the amount approved by the House. I urge you to fund these positions. We can have all of the technology and rules to protect the ports laid out in this law, but if we do not have people to man those positions, it will not do much good.

Conclusion

I appreciate the opportunity to express my thoughts on the SAFE Ports Act of 2006 on its one-year anniversary. I believe this was a good piece of legislation that can be improved with a few adjustments. I am available for any questions you may have.

Thank you.

Ms. SANCHEZ. I thank all the witnesses for their testimony.

I will remind each member that he or she will have 5 minutes to question the panel, and I will recognize myself for questions. I would like to start with Mr. McLaughlin.

In the earlier panel, we had Ms. Fanguy testify that there were only 70 denials on HAZMAT. You mentioned 5,500.

Mr. McLAUGHLIN. She said 70? I think she must have misspoke. The number I had was 5,500, and I met with TSA recently and they said 5,500.

Ms. SANCHEZ. Okay. My question for you is, you mentioned some of the problems that your membership has with the TWIC process, including loss of privacy. Can you sort of just give us an indication of what that means to them?

Mr. McLAUGHLIN. Well, I think that this committee held a hearing on the HAZMAT truck drivers, and one of the issues that was brought forward were some of the truck drivers were not applying because of that issue. They may have something in their past that is not a disqualifying offense, but they don't want somebody else to look at it, and therein lies—and I get calls from individuals that may have a background and it does not—those crimes do not fall into these categories, but they are still concerned. And they are concerned about the loss of privacy, they are concerned about where this information is going, who is looking at it, where it is being stored, all those questions that I get.

And there is just a concern out there that they are the ones that are losing their privacy, and you may have a longshoreman that does have a criminal background that comes to work every day with a big American flag on the back of his truck. And so you are saying that this person is a risk to the United States. And so the connection between a criminal background and a terrorism security risk, which is what MTSA—it is really difficult to look at the two and to make a determination, I think.

And, furthermore, we have taken a lot of, particularly in L.A.-Long Beach, a lot of young people recently that have come into the union that were from tough neighborhoods; and I worry about so easily taking away their livelihoods. Because they have a good job and a good chance to build a future with this union and with this job, and it should not be taken lightly.

It is a good job for women as well. I don't know if you knew this, but probably about 25 percent of the longshore workers in L.A.-Long Beach are women. So it is a good job for both men and women.

Ms. SANCHEZ. Thank you for clarifying that and putting that on the record. Because I think that these are jobs that pay well over the long run and people do get a second start in many cases towards working things out and providing for their families. We wanted to get that on the record.

Mr. Blanchet, according to your written testimony, a TWIC can be forged within 48 hours. What steps do you think TSA should be taking to prevent this from occurring? And should the readers be rolled out at the same time that the cards are?

Mr. BLANCHET. That is correct. The readers should already have been established. The system that is going to be in place is going to be status quo to the system you have today; and that is, go through the gate and show a driver's license. A majority of the trucks that enter the gates today are not physically examined by the guard. And what I mean by that, the guard is supposed to take the driver's license, look at the picture, and try to match it with the driver. That is not being done.

If you have a TWIC, you will have the same cosmetic issue as the driver's license. So until you have the biometric reader to read the information from the fingerprints to the face, to the card, you are not going to have anything which is secure. Homeland Security should be Homeland Scary.

Ms. SANCHEZ. Thank you.

I yield back. I will give 5 minutes to the ranking member.

Mr. SOUDER. I will try not to use my 5 minutes.

I had a question for Mr. McLaughlin first. Does the union get notified when someone is turned down? If they are a member—you said a lot of people get letters. They don't know how to do that?

Mr. MCLAUGHLIN. We haven't gotten any letters so far, but we don't have the rollout until mid-November. But, as far as I know, the union does not get notification that the individual is disqualified.

Mr. SOUDER. That will be something interesting to pursue. Because that would be another fallback protection for individuals. I mean, we want to keep people who are high risk out. I am a hard-liner on that question.

The question is, however, if folks are misidentified and we are having confusion at the grass roots and don't understand it, I would think that would be one additional union benefit, would be if the union also knew whether one of the members had been turned down.

Mr. MCLAUGHLIN. I will have to think about that, because I don't know an individual who would want the union to know what it is they got.

But I think one thing the union can do is educate them, expect within a certain amount of days you are going to get your card or please go to the union so we can help you. That is something that we are talking about doing now.

Mr. SOUDER. One of the things is I would assume that the union would know they were turned down because they will no longer be able to keep their job. So, to some degree, privacy—being turned down, if you can't show up to work is kind of non—you may not know the reason, and that is a legitimate concern with privacy laws.

Mr. MCLAUGHLIN. No. Because you are going to have the rollout, but the compliant date may be a year from now. So it may be up the road. So they may lose their window of opportunity to apply for a waiver. So they may lose that window of opportunity but still be allowed to work because the port is not compliant with TWIC card.

Mr. SOUDER. Mr. Koch and Ms. Alexander, in the 10 plus 2 initiative, which I take it you have serious concerns about because of it is being done in a room where you are not able to input and then all of a sudden it is there, I don't understand why things aren't floated and worked in a more cooperative way. But are there specific elements of the data that you are afraid of that aren't going to be necessarily important for targeting but you feel put additional paperwork? Where are your major concerns there?

Mr. KOCH. At this point, Congressman, we are not sure we have any concerns. We think the strategy is sound. We think the 10 plus 2 data elements that CBP has identified makes sense.

And, frankly, we commend CBP. They have been very open. They have reached out to the trade community, carriers, brokers, forwarders, importers for a year to get input and feedback. So I would expect that this proposed rulemaking, when it comes out, should surprise very few people.

Obviously, we need to wait and see what is in the NPRM, but our expectation is that it will be exactly as they have advertised and an important supplement and improvement to the risk targeting system that they presently use.

Mr. SOUDER. Do you agree with that, Ms. Alexander? You mentioned a closed room.

Ms. ALEXANDER. Well, the closed room I was talking about more for the GTX issue. On the 10 plus 2, there are various elements that have been requested that we do not collect data on right now or that we do not have ready access to. So what our big concern is that when this rolls out we will have time to establish the new processes within our company to be able to collect that data. That is our big concern. We assume that might take 1 year, 1-1/2 years to be able to collect all that data in the proper process.

Mr. SOUDER. Madam Chairwoman, I will yield back.

Ms. SANCHEZ. The members present have agreed to each ask one question so we can get through this process and close off this hearing so we can go over and vote since we have a vote on the floor.

At this time, I will acknowledge Mr. Green for his question.

Mr. GREEN. Thank you, Madam Chair.

And I want to thank all of the persons who are here to testify today, especially Mr. Battles. He happens to be from Houston, Texas, where we happen to have our port. I, along with Congressman Gene Green, had an opportunity to tour the port. We were impressed—I was—with the coordination center, the communications abilities that you have; and, also, I was impressed to find out that you have a public-private partnership called the Ship Channel Security District. And I would just ask if you would enlighten us as to how this public-private initiative is functioning.

Mr. BATTLES. Thank you, Congressman Green.

As we move forward in port security, what has happened is we first started looking at the individual security facilities. We have moved on now to a regional basis. Because each facility is inter-

related with the facility next to us, so the challenge became how do we have projects that include various facilities over a regional basis in addressing such issues as on-water security interoperability.

So we formed a partnership between Harris County and the Port Authority and the private sector, mostly the chemical plants that align the Houston Ship Channel; and we moved forward and we applied for security grants in both rounds five and six and were awarded, combined, about just under \$30 million. The challenge has been now that, once we have those funds, where do you get the operational and the maintenance funds to be able to operate those projects?

For example, one of the projects was on the water police capabilities for security on the water. Operating those boats becomes very expensive. So this past legislative session in Austin we had legislation passed that allowed us to form a security district. This is a self-taxing district where the members in the geographic boundaries of the security district come together, vote. They have to have 50 percent of their members vote for it, and then they will move forward and establish an equitable relationship to tax themselves to pay for O&M and also to move forward on providing the seed money that is necessary, the matching money for funds.

It also provides the vehicle to be able to evaluate projects on a much greater regional basis for the holistic good of the community, not only for business—I mean, not only for prevention and response but also now new focus on business continuity and on business continuing.

Ms. SANCHEZ. Thank you, Mr. Green.

I will now recognize Mr. McCaul for his question.

Mr. MCCAUL. I thank you, Madam Chair.

I had a specific question. I will be brief, given the time constraints.

Mr. KOCH AND MR. Battles, the 100 percent screening restriction or the provision that was put in the 9/11 bill, I was one of the conferees. We had a very healthy debate over this whole issue. But I am concerned about how it works in the real world as a practical matter, and if I could raise just a couple points that I heard that I think raise some concerns.

One is, who does the screening and in what foreign country are you doing the screening? Will China, for instance, allow us to do with screening with Customs or does China want to contract? Or you mentioned Dubai Ports. How feasible is this by 2012?

And then, secondly, if the reciprocity requirement is placed on the United States to inspect all of our exports, do we have the capability and the resources to do that, in your judgment?

Mr. KOCH. I think the questions you have raised are some of the same questions we have raised. We don't know how this would work in reality. We don't know that the governments abroad know how this is supposed to work in reality. The port operators abroad do know not how this is going to work in reality. There are simply too many fundamental issues that have not been raised or tackled or addressed either by the Congress in passing this or by DHS trying to digest what this means at the present time.

To some extent, a lot of people look at this and say, well, because the effective date is 2012, maybe we don't have to worry about it. I don't think that is the way other governments and the port community is looking at this. The United States is a leader on maritime security and port security issues, and it is important for the government to speak clearly so that we understand what the rules are going to be going forward.

As to resources, if we had to inspect 100 percent of our outbound containers similarly to what is talked about for inbound, there are not the resources to do it. As Mr. Battles said, the Port of Houston couldn't do it. It would be a severe problem for American exporters. The vision of a 100 percent container inspection is certainly an attractive vision, but I think a lot of work needs to be put into this to confront what are real-world problems that up to this point have not been addressed.

Mr. MCCAUL. I think it is an attractive vision, but I think we are going to have to work hard with you to determine we are going to do this.

Mr. Battles, just real quickly.

Mr. BATTLES. Yes, I concur. It is a huge challenge. And what we are trying to bring to light is a rationalization of let's not get lost on the methodology of how we are going to achieve our goal. Let's achieve our goal and use all of the resources that we have available to us, not necessarily get hung up on one particular issue where we want to have every container inspected overseas.

I think if we have a multitude of programs that layered on top of each other we will be able to achieve the goal of secure and safe ports but at the same time not put handcuffs on commerce and slow commerce down.

Mr. MCCAUL. Thank you, Madam Chair.

Ms. SANCHEZ. Ms. Jackson Lee, you are recognized for one question. We have a vote on the floor with less than 5 minutes to go.

Ms. JACKSON LEE. Let me spend time saying to Mr. Battles we thank you for your presence here today and to acknowledge my concern about some of the issues that you have raised.

We thank the witnesses for their presence.

Let me indicate to both unions that you will find very a very strong advocate for training. We will respond to your concern about the FBI list that may be inaccurate and, as well, we will respond to your concern about the communication process. That is very, very important; and I look forward to working with you specifically on that.

Mr. Battle, I would like you to comment on the lack of the reader, which I don't think most people understand that you are going to be in this program and you don't have a tested reader of the program for the TWIC card. And as you answer that, the question is embellished by the fact of you telling us how your unions in the Houston port are going to be involved in this security process.

Thank you for your presence here and the great work of the port that I have enjoyed working with.

Mr. BATTLES. As far as the reader is concerned, our concern is basically, number one, that we have a reader that works. It is going to be very, very challenging to be able to process the long-shoremen as they are standing in front of the turnstyle to go to

work every day. We don't want to hold them up. We have to come up with an efficient product.

If you look at the specifications as required in FIPS 201, it calls for a contact reader. And our concern is that in a marine environment, a contact reader will not last very long, that it will get misreads and it will slow down the process. So we are trying to move forward on a contactless reader that will incorporate the biometric requirement that the TWIC card is going to have.

As far as working with the union, we have always had a very strong working relationship with the union. The concern about a longshoreman being denied a TWIC card is a very, very serious issue. Denying a man or woman their livelihood should not be in any way taken so easily. So we are dedicated to work with the union, find solutions for it. But we have found that with proper processes and having the ability to appeal it that we hopefully feel that we will have a fair and equitable rollout of the TWIC card.

Ms. SANCHEZ. I thank the witnesses for their valuable testimony and the members for their questions. And the members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond quickly to those questions.

Hearing no further business, this subcommittee stands adjourned.

[Whereupon, at 4:37 p.m., the subcommittee was adjourned.]

Appendix A: Executive Summary of C-TPAT Partners Cost-Benefit Survey Prepared by the University of Virginia for U.S. Customs and Border Protection

II Executive Summary

C-TPAT Survey

- Of the 6,000 C-TPAT certified companies that were sent an invitation to participate in the survey, a total of 1,756 completed the survey (29.3%). Of the 1,756 responses received, 54.3% were received from importers, 20.6% from carriers, 17.8% from service providers, and 7.3% from foreign manufacturers. The percentage of responses received by enrollment sector closely mirrors the size of each enrollment sector relative to total program membership
- The Center for Survey Research (CSR) at the University of Virginia conducted the 2007 C-TPAT Benefit Cost Survey from January to April 2007.

C-TPAT Partners Profile

- Nearly three-quarters of these businesses are privately owned (74.0%), while another quarter are publicly owned (24.0%). The participating companies have been C-TPAT certified for 2.6 years on average.
- Six out of ten (62.1%) companies that participated in the C-TPAT survey indicated that their company's headquarters were located in the United States. The remaining companies reported that their headquarters were located in Canada (25.0%), in Mexico (3.2%), or in other countries (9.7%).
- Of the 953 importers who responded to the survey, 64% have been validated. Of the validated importers, 21.7% were classified as Tier 3, receiving the maximum level of benefits provided under the program.

Prior to joining C-TPAT

- Prior to joining C-TPAT, survey respondents in more than half (54.8%) of the businesses surveyed did not know about the protection programs or initiatives their companies have put in place. In addition, nearly half of the businesses (46.6%) did not have a formal system in place for assessing and managing supply risk.
- Slightly more than one-third (35.7%) of businesses had a formal system in place for assessing and managing supply chain risk. Furthermore, about 4 out of 10 businesses had no formal supply chain continuity and contingency plans.
- However, because of their participation in previous Customs and Border Protection programs, or due to their company's risk management processes, half (50.3%) of the businesses had implemented most or nearly all the C-TPAT program criteria prior to applying for membership.

Motivations for Joining C-TPAT

- For all businesses, "reducing the time and cost of getting cargo released by CBP" is the most important potential benefit, followed by "reduced time and cost in CBP secondary cargo inspection lines." Of all the potential benefits presented to businesses, "reducing insurance rates" was the lowest rated item.
- According to Importers, the most important motivation for them to join C-TPAT is to "to reduce the disruptions to the supply chain". For non-importers, 62% indicated that their principle reason for joining the program was that their business partners required them to be C-TPAT certified.

Potential C-TPAT Implementation and Maintenance Costs

- Of all the potential C-TPAT implementation costs, "improving or implementing physical security costs (doors, windows, electronic access, cameras, fences, gates, lighting, etc.)" received the most mentions. It was also the highest among all the potential implementation costs with an average of \$38,471.

- Of all the maintenance cost items, “maintaining physical security” and “maintaining in-house education, training, and awareness” received the most mentions by all the businesses.
- With respect to the average amount of money spent, “maintaining the use of security personnel” (\$40,441) and “salaries and expenses of personnel” (\$28,454) were the highest costs to maintain the C-TPAT program.
- The results of the survey also indicated that the ease of implementing the C-TPAT program criteria was found across all business types. Overall, 59.3% of Importers, 59.1% of Carriers, 62.0% of service providers, and 59.2% of manufacturers found that it was somewhat or very easy to implement the C-TPAT program criteria.
- During the last full year before they joined C-TPAT, Importers’ total annual expenditures on supply chain security averaged an amount of \$35,006. The estimated annual expenditures on supply chain averaged \$66,353 in 2005 and were projected to be \$77,997 and \$69,905 in 2006 and 2007.
- For Non-Importers, total annual expenditures on supply chain security follow a similar pattern as that of Importers, with the total annual expenditures on supply chain security averaging \$57,406 prior to joining C-TPAT. However, the 2007 projected expenditures (\$100,025) were higher than the 2006 projected expenditures (\$61,964).

Benefits of C-TPAT Participation

- Almost one-third (32.6%) of businesses said that the benefits outweighed the costs, while nearly one-quarter (24.2%) of businesses said that the C-TPAT benefits and the affiliated costs were about the same.
- For all businesses, the major impacts of their C-TPAT participation have been in the field of workforce security, time to release cargo by CBP, time in CBP inspection lines, and predictability in moving goods.
- More than one third (35.4%) of Importers reported that their participation in C-TPAT has decreased their number of U.S. Customs and Border Protection (CBP) inspections. In a follow-up question, these importers indicated that their number of CBP inspections decreased by more than half (51.7%).
- Importers that have been C-TPAT certified for a period of more than 3 years were more likely to say that their number of inspections have decreased (42.8%) because of the C-TPAT participation than were those Importers which have been C-TPAT certified for a period of 2 to 3 years (33.8%) or less than 2 years (27.1%).
- Importers said that their participation in C-TPAT has increased their supply chain visibility and nearly one quarter (24.3%) indicated that their participation in C-TPAT has increased their ability to predict lead-time. Nearly 3 out of 10 Importers (28.9%) reported that their participation in C-TPAT has decreased the disruptions in their supply chain.
- Of highway carriers, 41.5% reported that their participation in C-TPAT has decreased their wait times at the borders, while 44.4% said their wait times at the borders have stayed the same.
- More than two-thirds (68.7%) of non-Importers said that their number of customers has stayed the same, while 17.0% have reported that their participation in C-TPAT has increased their number of customers. About the same proportion of non-Importers (17.4%) also indicated their participation in C-TPAT has increased their sales revenues.
- Overall, since becoming C-TPAT certified, non-Importers who reported an increase in customers have gained 35.2% new customers. Non-Importers who reported an increase in sales indicated that their company’s sales have increased by 24.1%.

C-TPAT Impact on Risk Management

- The vast majority (81.3%) of businesses that had a formal system in place for assessing and managing supply risk agreed or somewhat agreed that their businesses’ ability to assess and manage supply risk has been strengthened as a result of joining C-TPAT.
- Three quarters (75.2%) of businesses that had formal supply continuity and contingency plans before joining C-TPAT reported that their supply continuity and contingency plans have been strengthened as a result of joining C-TPAT.

C-TPAT Supply Chain Security Conferences

- Nearly thirty percent of businesses (29.3%) said they have participated in Supply Chain Security conferences. The vast majority of the conferences’ participants (98.4%) reported that the conferences were valuable, with 37.2 percent rating them as extremely valuable and 42.2 percent rating them as valuable. About half (50.2%) of the businesses would like to have these C-TPAT Supply Chain Security conferences presented once a year.

- Nine out of ten (92.6%) businesses have contacted the C-TPAT program personnel and 81.5% of these businesses said that they have not experienced difficulties in obtaining responses to their questions or concerns. In addition, 83.8% of these businesses indicated that C-TPAT responses to their questions or concerns were provided in a timely fashion.

- Businesses also had a positive evaluation of their Supply Chain Security Specialist (SCSS). An overwhelming majority (98.3%) of businesses reported that their Supply Chain Security Specialist was very knowledgeable (54.1%), knowledgeable (34.4%), or somewhat knowledgeable (9.8%). Interestingly, this appreciation of the knowledge of the Supply Chain Security Specialist was across all businesses regardless of their type, size, or the number of years they have been C-TPAT certified.

Overall C-TPAT Evaluation

- More than half (56.8%) of businesses indicated that C-TPAT benefits outweighed the costs (32.6%) or the benefits and the costs were about the same (24.2%). Slightly more than one quarter (26.4%) reported that it was too early to compare the benefits and the costs.

- While more than one-third (38.4%) of businesses indicated that their management was concerned about the potential impact on cost when their companies were considering joining C-TPAT, the vast majority of businesses indicated they have never considered leaving the C-TPAT program (91.5%) and that they would definitely (78.1%) or probably (18.1%) stay in the program.

Appendix B: Additional Questions and Responses

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON
HOMELAND SECURITY

RESPONSES FROM STEPHEN L. CALDWELL



January 15, 2008

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

Subject: *Response to Post-Hearing Questions Regarding the SAFE Port Act*

Dear Mr. Chairman:

This letter responds to your request for additional information related to the Subcommittee on Border, Maritime and Global Counterterrorism's October 30, 2007, hearing on the SAFE Port Act and my testimony. Enclosed are our responses to the supplemental questions you submitted for the record.

If you have any further questions or would like to discuss any of these areas in more detail, I can be reached at (202) 512-9610 or caldwells@gao.gov.

Sincerely yours,


Stephen L. Caldwell

Director
Homeland Security and Justice Issues

Enclosure - 1

Post-Hearing Questions for the Record
From Representative Bennie G. Thompson, Chairman of the
Committee on Homeland Security, U.S. House of Representatives
Hearing on
“SAFE Port Act: Status and Implementation One Year Later”
October 30, 2007

Interagency Port Operations Centers

1. In your testimony, you referenced several challenges to improved information sharing efforts, including the lack of clearances and overlapping responsibility. What steps should DHS take to fix these problems?

Answer:

As recently as last October we reported that the Department of Homeland Security and the Department of Justice were working to improve and clarify the ability of state and local homeland security officials to receive security clearances, but that challenges persist.¹ The time to receive a clearance from the FBI has gone down. For example, according to the FBI, Top Secret security clearances granted by the FBI to state and local personnel in March 2007 took an average of 63 days to complete, down from an average of 116 days in fiscal year 2006. The FBI is also taking actions to further reduce the time needed to issue clearances, such as prioritizing background investigations for state and local officials and facilitating the electronic submission of fingerprints. One of the major challenges, however, is the ability of state and local personnel accessing classified material was federal agencies not accepting clearances granted by other federal agencies. A DHS official acknowledged to GAO that, overall, federal agencies do not have a consolidated system for granting and handling security clearances and said that currently there are not sufficient federal efforts to develop such a system. Developing such a consolidated system may be helpful in furthering the ability of state and local security officials in obtaining access to classified information.

The federal government has also taken action to reduce overlapping responsibilities in dealing with maritime threats, but these efforts could also be expanded. The Maritime Operational Threat Response (MOTR) Plan was issued in October 2006 and set a general framework for coordinating federal agencies in the event of a maritime threat. The MOTR Protocols, first released in April 2006, laid out the specific federal participants, coordinating activities, and conferencing procedures to facilitate a unified federal response with delineated responsibilities to the threat at the national level. The Protocols called for engagement with affected state and local level

¹GAO, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35 (Washington, D.C.: October 30, 2007).

stakeholders through such mechanisms as Joint Terrorism Task Forces or Port Security Committees, but does not lay out the formal means for engaging and coordinating with local agencies at the threatened location. Expanding the scope of the protocols to the local level could help alleviate coordination issues on scene.

International Port Security Program

2. According to your testimony, the Coast Guard has occasionally encountered initial reluctance by some countries to allow Coast Guard officers to visit their ports due to concerns over sovereignty. In your opinion, how does this impact the success of the program?

Answer:

Overall, the Coast Guard has gained access to visit nearly all of the countries it intended to through the program. Cooperation of some countries was gained through the use of the reciprocal visit feature of the program through which countries can visit the United States and observe security measures at U.S. ports. In some cases, countries visited U.S. ports before the Coast Guard visited the countries' ports. However, concerns over sovereignty by some countries still has had some impact on the timing and locations of the Coast Guard's visits as the Coast Guard can only visit facilities they are granted access to by the countries and at the times designated by the countries. As a result, there is the potential that what the Coast Guard observes at those facilities and at those times may not necessarily be the normal security posture for that facility or country. However, under any circumstances, the visits only provide a snapshot of the security at a port at that point in time. In commenting on our work on port security in the Caribbean Basin, the State Department noted that compliance with the ISPS Code does not necessarily mean the port is secure from a terrorist attack. In that work, the State Department stated that it and its contractors have witnessed open gates, poor screening of vehicles, and inadequate physical protections at ports with cruise line activity. We are in the process of evaluating the Coast Guard's International Port Security Program and plan to report on our findings in February 2008.

Port Security Exercises and Training

3. What steps should the Department take to implement a successful training and exercise program?

Answer:

While GAO has not specifically outlined the steps for a training and exercise program, we have noted certain practices in previous work that the Department could consider when designing a program. These practices include:

- **Completing Timely and Substantive After Action Reports (AAR):** GAO's analysis of past exercises reported on the importance of producing timely AARs, noting that in order to ensure that individual agencies learn lessons after each federal counterterrorism exercise, agencies should prepare a timely AAR or other evaluation that documents the results. Untimely AARs can negatively impact the effectiveness of exercises because information may not be available for incorporation into future exercises. Similarly, if AARs lack sufficient fundamental content, they cannot be used effectively to plan exercises and make necessary revisions to programs and protocols.
 - **Tracking and Implementing Lessons Learned:** Our previous work on Hurricane Katrina illustrated the consequences of applying or not applying lessons learned from training exercises. The 2004 "Hurricane Pam" exercise, sponsored by FEMA, was designed to develop a response and recovery plan for a major hurricane that floods New Orleans and the surrounding parishes and to identify any issues that could not be resolved based on current capabilities. The Hurricane Pam exercise anticipated many of the events transpiring as a result of Hurricane Katrina and while the exercise resulted in some action, other lessons were not acted upon despite recognition that the exercise reflected the dangers of a serious hurricane striking New Orleans.
 - **Exercising a Variety of Scenarios:** In our past work, we found that that Coast Guard terrorism exercises frequently focused on prevention and awareness, but often did not include recovery activities. It will be important that future exercises also focus on recovery operations so public and private stakeholders can cover gaps that might hinder commerce after a port incident.
 - **Including Key Jurisdictional Players:** According to the Coast Guard, as the primary sponsor of many maritime exercise programs, it faces a continuing challenge in getting comprehensive exercise participation. Coast Guard terrorism exercises we have reviewed in the past have raised concerns about the coordination of resources as well as jurisdictional or decision making authority—concerns that can only be addressed when key agency players are involved in the exercise.
4. In your written testimony, you state that maritime security exercises would benefit from timely and complete after-action reports, increased collaboration across federal agencies, and broader port-level coordination. Why is this so important?

Answer:

Complete and timely analyses of maritime security exercises represent an important opportunity to identify and correct barriers to a successful response. The inability to

consistently report on exercises in a timely and complete manner represents a lost opportunity to share potentially valuable information. Analysis of after-action reports presents an opportunity to identify potential barriers to an effective response during an actual threat or incident. These reports can also provide valuable input for future exercises. In previous reviews of exercises conducted by the Coast Guard and others, we found that timely after-action reports were necessary to help ensure that potential lessons can be learned and applied to each counterterrorism exercise. Additionally, if after-action reports do not contain certain fundamental content, such as a listing of exercise objectives and an assessment of each of these objectives, they cannot be used effectively to plan exercises and make necessary revisions to programs and protocols.

A successful response to a terrorist threat or incident in a seaport environment requires the effective cooperation and coordination of numerous federal, state, local, and private entities—issues that exercises and after-action reports are intended to identify. Responding effectively in such exercise scenarios can be difficult. Depending on the nature of the incident and the particular port involved, dozens of federal, state, and local agencies may be involved. The incident may also require close coordination across many jurisdictions, raising issues about who has authority or how agency personnel can communicate effectively when they have different chains of command. A properly designed, executed, and evaluated exercise can clarify roles and responsibilities between and within response units and organizations as well as improve cooperation among private sector organizations and government agencies. However, according to the Coast Guard, exercises face a continuing challenge in getting comprehensive participation from relevant agencies. Lack of participation and collaboration may limit the lessons learned and potentially affect the cohesion of a future response.

Recovery Plan

5. According to your testimony, the Coast Guard has issued limited instruction and assistance for developing procedures to address recovery situations. How would this instruction and assistance benefit the port stakeholder?

Answer:

Although we discussed this issue briefly in our written statement, we were unable to go into much detail because of its sensitive nature. A more thorough discussion can be found on pages 36-42 of our October 2007 restricted report *Maritime Security: Further Port Security Efforts Needed to Address Resource and Commerce Challenges* (GAO-08-111SU). Copies of this report were provided to the staff of the Homeland Security Committee and additional copies can be provided upon request.

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

RESPONSES FROM MAURINE FANGUY

Question 1.: According to Mr. Battles, TSA underestimated the TWIC numbers at the Port of Houston by 320,000. Similar problems occurred at the Ports of New York and New Jersey and Savannah). **Who came up with the original numbers and how much did you pay them?**

Response: The Transportation Security Administration (TSA) Office of Finance and Administration led the effort to develop the original population estimates, with contractor support from International Business Machines Corporation (IBM). The estimated cost for this support is \$48,000. In developing this estimate, TSA consulted with the following government and industry authorities: United States (US) Department of Transportation/US Maritime Administration, Army Corps of Engineers (Waterborne Commerce), Journal of Commerce, American Association of Port Authorities, Bureau of Transportation Statistics, A. Strauss-Wieder Inc., Martin Associates, Economic Research Associates, International Longshoremen's Association, International Longshore and Warehouse Union, United States Maritime Alliance, Pacific Maritime Association, American Waterways Operators, Maersk, Wallenius-Wilhelmsen, American Trucking Association, Owner-Operator Independent Drivers Association, International Brotherhood of Teamsters (Port Division), US Census (Vehicle Information), University of Michigan, University of Minnesota, California State University at Long Beach, University of Central Florida, American Shipbuilding Association, Shipbuilders Council of America, Cruise Industry News, International Council of Cruise Lines, Minerals Management Service, National Ocean Industries

Association, Independent Petroleum Association of America, American Petroleum Institute, and the National Petrochemical and Refiners Association.

TSA is continually working with the United States Coast Guard and industry stakeholders to gather additional data on the maritime population. However, there is sufficient flexibility and capacity in the system to accommodate unforeseen fluctuations in the population.

Question 2.: The TWIC was supposed to be the one card that provided uniformity and consistency. **What steps has TSA taken to pre-empt state access cards like those issued in Florida?**

Response: Under the final rule published on January 25, 2007, States are not preempted from instituting their own background checks or badging systems in addition to the Transportation Worker Identification Credential. We note that a State may be the proprietor of ports or port facilities, and, as the proprietor, is free to set standards for who may enter onto their facilities, as does any other proprietor. In addition, States may have set standards for reasons other than guarding against the threat of terrorism, such as to combat drug smuggling or organized crime. As such they are not regulating in the areas that DHS is regulating.

Question 3.: TSA contractors have already lost two computers containing personal information. **Are you confident that TSA has taken the proper steps to secure the TWIC computers?**

Response: Transportation Security Administration (TSA) takes data security very seriously. TSA and its contractors are committed to maintaining the privacy of personal information and take many precautions to protect it. The Transportation Worker Identification Credential (TWIC) system incorporates a 256-bit Advanced Encryption Standard for whole disk encryption on all enrollment workstations, encryption of the enrollment package during transmission through a virtual private network, and encryption of the data in the TWIC system, which is located at a secure government facility. This standard is a National Institute of Standards and Technology standard that is approved by the National Security Agency for the transmission of Top Secret information and reflects Federal Information Processing Standard 197. TSA recognizes that data security is an ongoing process, and will continue to monitor our systems and practices to enhance the security of personal information.

Question 4.: We have been told repeatedly that TSA has failed to notify and educate port stakeholders about TWIC. **What steps are you going to take to fix this problem?**

Response: The Transportation Worker Identification Credential (TWIC) Stakeholder Communications Committee is comprised of approximately 35 industry and labor representatives and has held 6 meetings to date. These meetings are well attended, useful information is presented and distributed to the membership and valuable feedback is received from the membership. To illustrate the effectiveness of this committee, membership requests continue to be received from stakeholders interested in participating. We are very pleased with the workings of this committee, the two way flow of information it fosters, and participation from industry.

Additionally, as cited in recent Government Accountability Office (GAO) testimony (October 31, 2007 to the Committee on Homeland Security, House of Representatives), the Transportation Security Administration (TSA) has taken steps to address previous GAO recommendations regarding improving communications and coordination with maritime stakeholders, including posting frequently asked questions, participating in numerous conferences and briefings, conducting outreach with maritime facility operators and port authorities, and disseminating informational bulletins and fliers. The testimony states that stakeholders from the Ports of Wilmington, Delaware, Los Angeles, California and the Maritime Exchange of the Delaware River and Bay Authority, with whom GAO spoke in October 2007, stated that TSA and its enrollment contractor have placed a greater emphasis on communicating and coordinating with stakeholders and on correcting past problems. An official from the Port of Wilmington stated that, thus far, communication, coordination, and outreach by TSA and its enrollment contractor have been excellent and far better than during TWIC testing.

Question 5.: **When is TSA going to implement the reader pilot?**

Response: Vendors are currently developing contactless readers to operate with the Transportation Worker Identification Credential. After independently testing the readers for compliance with the specification, we plan to deploy readers at test sites early in calendar year 2008 and begin gathering test data. Delivery of the final pilot test report is scheduled for December 2008. The test will extend through 2008

to achieve all test objectives. However, the test is structured to provide data early in the pilot and throughout the test.

Question: The SAFE Port Act required a pilot program on the TWIC readers. The Department has decided to fund this program through the Port Security Grant program, although this was not required in the law. The pilot participants recently sent Mr. Chertoff a letter asking him to waive the 25% cost-share requirement for the pilots since all other TWIC pilots were fully funded by the government and he has the authority under MTSA to waive the cost-share. **What is Mr. Chertoff's position on waiving the 25% cost-share on TWIC reader pilots?**

Response: Currently DHS is reviewing the wavier request for the TWIC readers and a decision will be made in the near future.

Question 7.: The Port Security Grant program is already providing funds for TWIC implementation. **A key problem in determining costs are some policy decisions that DHS has yet to make. Three key ones are: (1) will all facilities be required to have use TWIC card reader; (2) At what MARSEC level and rates will facilities be required to have biometric checks, and (3) Will facilities be required to conduct PIN verifications and at what MARSEC levels? What is DHS' timeframe for making some of these policy decisions in light of the funding from the Port Security Grant program?**

Response: The specific policy decisions discussed in the question will be promulgated in a notice and comment rulemaking addressing Transportation Worker Identification Credential (TWIC) reader requirements for regulated vessels and facilities. The policy decision will be proposed in a Notice of Proposed Rulemaking, which will give regulated industry an indication of Department of Homeland Security (DHS) direction. However, decisions will not be finalized in a rule until a public comment period and TWIC pilot test of the business processes, technology, and impacts is completed. DHS intends to address these policy decisions by the SAFE Port Act deadline of April, 2009.

Regarding TWIC funding from the Port Security Grant program, approved applicants have up to 30 months from the grant award date to obligate their funds, providing sufficient time to implement TWIC reader projects given regulatory requirements.

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

RESPONSES FROM VAYL OXFORD

Question 1.: Section 121 of the SAFE Port Act states that DHS will produce a strategy for deployment of domestic radiation detection and imaging systems. When radiation portal monitors were first employed at ports, their installation was slowed by a failure of DHS/DOE and their contractors to work up front with ports to make sure the operating procedures and footprints would be complementary to port operations.

(Director Oxford, DNDO) Please explain if and how you included ports in the development of the strategy on domestic radiation detection and imaging systems required under Section 121 of the SAFE Port Act.

Response: CBP and DNDO have continued to work directly with all affected stakeholders to ensure that current business models are not negatively impacted by deployments of radiation portal monitor (RPM) or non-intrusive inspection (NII) equipment at field locations. Additionally, as a general practice, CBP and DNDO work with the port authority and other affected stakeholders to proactively schedule construction to coincide with any other activities at the port. This helps prevent scheduling delays and expedites the deployment process overall.

Question 2.: (Director Oxford, DNDO) **How are the Departments of Homeland Security and Energy and their vendors working with ports to ensure that the next generation of scanning technology will be complementary to port operations, including those being tested overseas as part of the Secure Freight Initiative?**

Response: Due to sovereignty concerns, CSI cannot set standards in a foreign country for the purchase and deployment of NII systems. However, it is recommended that host nation counterparts purchase NII systems that follow the guidelines of the World Customs Organization (WCO) Customs Compendium, Container Scanning Equipment, Guidelines to Members on Administrative Considerations of Purchase and Operation. Moreover, this language has been included in all Declarations of Principles signed from May 2005 and beyond. It should be noted that as a requirement for participating in CSI, foreign governments must purchase

their own NII equipment and that equipment must either meet or exceed the capability of NII equipment used by CBP domestically.

CBP, DOE, and DNDO continue to work with terminal/port operators to determine if NII and radiation detection equipment deployments are impacting trade and the flow of cargo at foreign ports. DHS and DOE also routinely meet with Secure Freight Initiative (SFI) partners to discuss SFI deployments and their effects on the flow of cargo. As discussions with stakeholders continue, these metrics will be expanded, readjusted, and supplemented.

Prior to deploying NII or radiation detection equipment, a complete site survey is conducted at the proposed site. During this survey port /terminal operators and other affected stakeholders are encouraged to participate and provide input. All stakeholders are given the opportunity to provide input into final designs. Deployment activities do not commence until all stakeholder concerns and input have been addressed and satisfied.

Question 3.: (Director Oxford, DNDO) The SAFE Port act also states that Department shall publish technical capability standards and recommend standard operating procedures for the use of non-intrusive imaging and radiation detection equipment in the U.S. **Can you give us the status of that requirement and how have you involved ports?**

Response: In accordance with Section 121 (f) of the SAFE Port Act, DNDO, in collaboration with the National Institute of Standards and Technology (NIST), shall publish technical capability standards for the use of NII and radiation detection equipment in the United States. Because Section 121 (f) requires such standards to take into account relevant standards and procedures utilized by other Federal department or agencies as well as those developed by international bodies, NIST is presently conducting a study of the detection capabilities required by existing national and international consensus standards for radiological and nuclear detection. NIST is scheduled to complete this study of the current standards baseline and provide DNDO a written report by the end of January 2008. NIST will then assist DNDO in convening an inter-agency working group of radiological, nuclear, and NII detection experts to develop threat-based government unique technical capability standards. DNDO plans to involve ports through CBP participation in this inter-agency working group.

Question 4.: (Director Oxford, DNDO) One concern is that Department has spent a lot of time and energy on the detection side, but not as much on remediation when an alarm goes off. Often the suspect container is taken to an off-site location, sometimes through a busy neighborhood, or it sits on the port without any protection or shield. **Can you give yourself a grade on your reaction to an alarm both in terms of immediate protection of the port and response if a problem was real?**

Response: The U.S. Department of Homeland Security has indeed focused significant attention upon the detection challenge because this is technically the more difficult element. But the Department recognizes that establishing and maintaining a systematic, comprehensive screening, interdiction and response capability requires that:

- The domestic program must be integrated with the Container Security or Secure Freight Initiatives elements which provide for intelligence collection, advanced screening, and timely notification.
- All points of potential entry must be covered using comprehensive, layered enforcement measures implemented by trained, qualified personnel.
- State-of-the-art equipment that is capable of detecting small quantities of threat material must be provided and used correctly.
- Detection equipment that is deployed is always accompanied by training on technical adjudication of alarms and associated response protocols.
- Systematic, effective measures must be in place to identify and secure threat materials.
- Appropriate and timely notifications must be made using an established system to allow effective command decisions and responses.
- The system must be probed and evaluated to assure continued readiness.

The Department has established U.S. Customs and Border Protection (CBP), along with the U.S. Coast Guard and the Transportation and Safety Administration (TSA), as the three agencies within DHS responsible for operational activities. These agencies integrate their interdiction activities, and work closely with other key agencies such as the Federal Bureau of Investigation on intelligence and the Federal Emergency Management Agency on emergency response.

Inspection and interdiction at ports of entry falls under the primary jurisdiction of the CBP. CBP has the immediate lead on reaction to an alarm both in terms of

immediate protection of the port and initial response if a problem were real (i.e., if a nuclear or radiological device or materials were to enter a U.S. port). It is probable that CBP will identify the conveyance/container with the threat material as high risk before arrival (i.e., at the point of embarkation or while offshore). If so, it may be screened or imaged at the port of embarkation through cooperative programs with CBP (e.g., Container Security or Secure Freight Initiatives) or while on shipboard by the Coast Guard.

For threat materials not identified and interdicted offshore, the next line of defense is detection in America's ports. All high-risk containers/conveyances are physically examined or scanned using imaging equipment and all are scanned for radiological materials using radiation detection equipment such as a radiation portal monitor (RPM) or the radiation isotope identification device (RIID). Scanning is done as early in the process as reasonable, in some cases on the dock shortly after the container is grounded, but is always done before the container leaves the port of entry.

When a CBP Officer identifies potential threat materials in a conveyance or container using radiation detection equipment, the officer contacts Laboratories and Scientific Services (LSS) via the National Law Enforcement Communications Center (NLECC). In the majority of cases, LSS has immediate access to the same data which the field CBP Officer sees by use of the Port Radiation Inspection, Detection and Evaluation (PRIDE) system; otherwise, the data is transferred electronically to LSS.

CBP has initial tactical responsibility in responding to potential threats at a port of entry. CBP will immediately isolate the container in an on-port secondary hold area, following the guidance of the CBP Standard Operating Procedure (SOP) for that port of entry. The container and area are secured; other conveyances are moved away from the isolated conveyance and additional conveyances/persons are not allowed to approach.

LSS provides recommendations on further diagnosis to confirm the existence of a threat. Measures may include additional imaging, additional spectra acquisition or other responses appropriate to the specific characteristics of the potential threat.

If LSS determines that there is potential threat material, they will contact the DNDO's Secondary Reachback team, comprised of national laboratory scientists, for additional expert advice and verification of threat. If appropriate, LSS scientists are dispatched from the regional office or a Radiological Assistance Program (RAP) team, comprised of regionally located national laboratory experts, may also be dispatched to the port to assist in confirming the diagnosis and to provide recommendations on remediation.

Upon reaching a consensus of a threat being present, LSS notifies the CBP Situation Room (SR) of the event, which escalates the event to appropriate DHS managers and entities (e.g., upper CBP managers, the CBP Office of Anti-Terrorism, the Domestic Nuclear Detection Office (DNDO) Joint Analysis Center (JAC), etc.). The SR and the JAC will notify the DHS National Operations Center (NOC) of the incident. Tactical command is elevated. The NOC activates the Federal Bureau of Investigation (FBI). Tactical command is transferred to the FBI once FBI Agents arrive at the port.

If warranted and in consultation with the FBI, various emergency measures can be put into effect or Port Emergency Preparedness Plan can be activated and/or Continuity of Operations Plans can be implemented, providing for notifications following contact procedures such that local emergency response authorities can initiate appropriate measures such as port closure, evacuation and stabilization.

With over 195,000,000 conveyances screened and 1,100,000 alarms resolved, DHS has proven operational experience which has provided feedback to refine the current system. The system is routinely tested. 'Red teams' challenge it by attempting to smuggle threat materials. Large scale drills, such as the recent TOPOFF4 exercise held in October of 2007 in Portland, test the effectiveness of the command and control systems for a radiological emergency. Based on the results of the various tests and exercise the Department judges that substantial measures are in place, and that continued efforts are appropriately focused on deploying detection equipment, on improving detection technology, and on continuing to train and test to refine the command and control structure.

As to assigning a grade, protection against use of weapons of mass destruction by terrorists on American soil has only one acceptable grade, A+. Although a great deal has been accomplished and the risk dramatically reduced, much remains to be accomplished. The Department continues to strive to attain the disciplined, comprehensive, systematic command and control structure needed to assure America is protected.

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON
HOMELAND SECURITY

RESPONSES FROM CAPTAIN FRANCIS STURM

Question 1.: What is the status of Coast Guard's progress monitoring compliance of facility security plans? What deficiencies have been found and what do they say about the status of our maritime security?

Are there enough facility inspectors and are they trained well enough to conduct facility inspections? Are there still going to be enough with the more stringent requirements under the SAFE Port Act-two inspections a year including one unannounced inspection?

Response: To date for 2007, the Coast Guard has performed in excess of 9,000 compliance checks of regulated facilities, thereby meeting the SAFE Port Act mandates. This number includes scheduled annual inspections and unannounced spot checks. Deficiencies generally relate to facility access control, monitoring and training.

Yes, the Coast Guard has the personnel resources in place needed to meet SAFE Port Act requirements. Additional funding provided in the 2007 DHS Appropriations Act allowed the Coast Guard to deploy an additional 39 facility inspectors to the field. The Coast Guard is also reviewing its training program for the inspector qualification to efficacy with position responsibilities.

Question 2.: Information sharing at the ports is a large undertaking, as well as an expensive undertaking. Given limited resources available, what are the next steps and should these be prioritized to ensure information is shared quickly and effectively, while also meeting concerns regarding rights of privacy and proprietary information?

Response: The Coast Guard is committed to sharing information in ports and views this functionality as a critical issue. To this end, beyond structural initiatives such as Area Maritime Security Committees, we have developed the web-based Homeport portal (<http://Homeport.uscg.mil>).

Homeport currently meets numerous Coast Guard needs for making information available via the internet. Homeport is the only CG Internet System certified for Sensitive But Unclassified (SBU) information, including Sensitive Security Information (SSI) as directed by 49 CFR 1520. Its functionality consists of four major areas (categories) of communication needs. The first is static web pages for all Coast Guard Sector commands and all components/departments at each Sector, similar to *www.uscg.mil*, as well as a web presence for numerous Headquarters Offices and Headquarters Units responsible for accomplishing a variety of Marine Safety and Security missions. This information is available to anyone with Internet access and does not require a Homeport user account for access.

Second, Homeport provides a web presence for providing information targeted for specific users or groups of users based on their role in both the public and private sectors of the global maritime industry and interests within each Sector Command's Area of Responsibilities (AOR). A Homeport user account is needed for access to this type of information. Requests for Homeport user accounts are reviewed and vetted locally at each Coast Guard Sector Command. The primary audience for this type of information is the Area Maritime Security Committees (AMSC), which are headed by the USCG Sector Commanders under their role as the Federal Maritime Security Coordinator (FMSC) for their AMSC. Other groups of users include a variety of both safety and security related committees, with members from both the public and private sectors.

Third, Homeport provides a collaboration feature in the form of Collaboration Communities that are organized by specific functional areas and types of content. Access to each Collaboration Community is controlled by the owner of that community. While , a Homeport user account is not needed to gain access, the Community owner has the ability to determine who has access to the information and can also set the access level (no-access, read-only, read-publish).

Finally, the Alert Warning System (AWS) application enables the Coast Guard to rapidly and reliably transmit targeted messages in bulk to maritime security partners and stakeholders. The system leverages the Homeport account management system to centralize user accounts and minimize account management requirements. AWS is the Coast Guard's official system for disseminating alerts, threat warnings, and other critical information to key partners and stakeholders primarily in support of maritime security related activities. It provides an efficient means of meeting the requirements of Title 33, Code of Federal Regulations (CFR), Subchapter H (requires Captains of the Port (COTP) to communicate MARSEC level changes through local Broadcast Notice to Mariners, and electronic means, if avail-

able, or as detailed in the Area Maritime Security Plan). AWS is a powerful communications tool capable of supporting and authorized for use to support a broad range of Coast Guard missions beyond maritime security such as hurricane preparedness and response, natural disasters and other critical and non-critical events necessitating timely port-wide notification.

Question 3: Granting security clearances to those with a need to know is a long-standing issue. **Does a ship operator or chemical plant manager having a clearance or not having a clearance really affect our nation's ability to use intelligence and tell port stakeholders to increase their security?**

Response: The need for such individuals to possess security clearances (i.e. Secret, Top Secret etc) would only become necessary if the information to be released was classified. In exigent circumstances, the Federal Maritime Security Coordinator (FMSC) may need to provide direction or share information with targeted industry stakeholders to prevent or mitigate threats.

The FMSC is not restricted from notifying port stakeholders of a need to increase their facility or vessel's security due to an individual not having a security clearance. If the Maritime Security (MARSEC) level of a port is raised, the change in MARSEC can be announced publicly. The specific security measures implemented by the facility or vessel operator would be dependent upon the approved vessel or facility security plan in place at that time.

However, if the FMSC has specific, targeted intelligence or is requiring a specific security procedure to be implemented (i.e. increase passenger screenings to 50%) then that information would only be released on a need to know basis. In accordance with Transportation Security Administration (TSA) rules, the individual to whom the FMSC is disclosing Sensitive Security Information would need to have completed a "Non-Disclosure Agreement" prior to the information being released.

Question 4: What will the Coast Guard having interagency operational centers do to increase our nation's security that isn't already occurring at our ports? What specific gaps in port security will these centers address?

Response: While there is currently a great deal of coordination and interaction between the Coast Guard and our port partners through the various Area Committees and Area Maritime Security Committees, the level of visibility and ability to monitor the wide range of port activities must be improved to elevate the level of maritime domain awareness in seaports. Interagency Operations Center (IOC) capability will address these gaps by establishing integrated operational protocols and business practices, and facilitating greater information-sharing among state, local and Federal port partners. The robust information-sharing, increased maritime domain awareness and operational coordination capability provided by IOCs will allow more effective all-hazards preparedness and response through efficient allocation and coordination of resources across the entire spectrum of port partner capabilities.

Question 5: While Operation SeaHawk in Charleston is one of the most advanced of interagency operations centers, the Department of Justice does not have plans to continue funding it. **What are the plans for the future of Operation SeaHawk**

Response: The Department of Homeland Security and the Department of Justice are working on transition options including identification of resource requirements, port partner participation and a projected timeline. Although no specific transition details have been developed at this time, the Department of Justice is not requesting funding for Seahawk. However, sufficient funds remain from the original appropriation of \$27 million to continue the project through FY 2009.

Question 6: Per Section 108 of the Safe Port Act, the Secretary was directed to establish interagency operational centers for port security within three years of enactment of the Act. **What progress has been made towards identifying relevant capabilities and solutions, many of which exist today within industry, to meet this requirement?**

Response: The Coast Guard has partnered with DHS Science and Technology (S&T) to conduct several pilots designed to inform operating requirements development and identify commercially-available technologies that will close critical capability gaps in Command and Control (C2), Information Management (IM) and Situational Awareness (SA). Pilot programs currently underway include the Visualization Tools pilot which is contracted to Mariner Group and installed in Sector Miami; Automated Scene Understanding (ASU) which is contracted to BAE Systems and installed at Sector Hampton Roads; and the Hawkeye System which is contracted to Northrop Grumman and installed in six Coast Guard Sector Command Centers.

Question 7.: While additional funding has yet to be provided for joint operation centers, it is important for the U.S. Coast Guard to work closely with ports to design these centers in a way that is compatible with port authority operation centers. **How does Coast Guard plan to coordinate and evaluate the design and operational requirements of these design centers once funding is made available?**

Response: The Coast Guard has a close working relationship with our port partners through the Area Maritime Security Committee (AMSC). Using input from the AMSC and informed by daily interactions with other port authorities, the Coast Guard will identify functional requirements, and through the Coast Guard's Facilities Design and Construction Center (FDCC), will develop design specifications that meet the unique needs of each port.

Question 8.: Given available resources, to what extent will CG perform inspections at each ISPS regulated facility? How will the Coast Guard determine which facilities are inspected?

Response: The Maritime Transportation Security Act of 2002 (MTSA) required the Secretary to "assess the effectiveness of the antiterrorism measures maintained. . .at a foreign port [that trades with the United States]." To implement this requirement, the Coast Guard has created the International Port Security Program. Because it is not practical to visit every facility of every country that trades with the United States, the program is designed to evaluate the country's implementation of the International Ship and Port Facility Security (ISPS) Code by visiting a representative sample of large, medium, and small ISPS-Code regulated facilities that reflect trading patterns of the country with the U.S. Government. The size of the sample varies with the country's size, results of the first assessment conducted, and risk factors such as the presence or absence of good governance indicators. In drafting the list of facilities to be visited, the Coast Guard places an emphasis on visiting those facilities that have direct trade with the U.S. Government.

Question 9.: Does the Coast Guard have enough fully trained and experienced personnel to effectively complete visits to facilities in approximately 150 countries by March 2008?

Response: Yes. The FY 2007 Department of Homeland Security Appropriations Act funded an additional 32 billets for the International Port Security (IPS) Program. The IPS Program is incorporating additional training opportunities for these new personnel to help bridge the initial training and experience gap. The increase in personnel will allow the IPS Program to complete visits to all of the United States' trading partners (approximately 150 countries) by March 2008.

Question 10.: Based on visiting countries (in most cases) only once every two years, how confident is the Coast Guard that facilities in ISPS-signatories are maintaining compliance with ISPS?

Response: In addition to the formal country visits, the International Port Security (IPS) Program's International Port Security Liaison Officers (IPSLOs) make annual visits to the countries in their respective portfolios and serve as the point of contact to maintain a continuous dialogue on port security issues. The IPS Program also culls information from other sources and continues to seek out additional information to provide an awareness of the International Ship and Port Facility Security (ISPS) Code implementation at facilities in ISPS Code signatory countries. These additional actions to monitor and engage with countries outside of the formal country visits equip the IPS Program to evaluate whether countries are maintaining compliance with the ISPS Code.

Question 11.: What are Coast Guard personnel finding during visits to facilities in other countries?

Response: Most countries and ports are eager to showcase their port security practices and International Ship and Port Facility Security (ISPS) Code implementation. In many countries, the Coast Guard finds physical security is usually adequate. The most frequent areas of major non-compliance observed are access control measures, drills and exercises, and training programs. Additionally, maintaining compliance with the ISPS Code can be a challenge for some countries due to associated implementation expenses or not having an adequate auditing capability at the national level.

Question 12.: What has Coast Guard determined will be the impact of rotation length for International Port Security Program personnel, given the training and experience needed for effective observations of facility security during country visits

Response: There is no particularly unique challenge being faced beyond training issues that affect the Coast Guard in general during the normal rotation process. There are sufficient program personnel to accommodate regular rotations while maintaining appropriate competency levels. Additionally, the International Port Security Program has increased the number of its civil service personnel to maintain continuity and experience during military rotations.

Question 13.: Has the Coast Guard established the Port Security Training and Exercise Programs required by the SAFE Port Act? It is our understanding that port workers still lack the necessary training.

Response: The Coast Guard sponsors the Area Maritime Security Training and Exercise Program, and assists the Transportation Security Agency (TSA) with their port security exercise program. In 2006, the CG and TSA collectively sponsored 53 port security exercises.

The Coast Guard is also supporting the Federal Emergency Management Agency (FEMA) National Preparedness Directorate's National Integration Center (formerly known as the Office of Grants and Training Division), through training and exercise integration, to implement additional SAFE Port Act training requirements. Notably, the Office of Grants and Training has awarded a \$6.18 million Cooperative grant to Florida State University to develop courses meeting Maritime Transportation Security Act (MTSA) of 2002 requirements, and covering the eight port security-related topics required under the SAFE Port Act.

Additionally, the Coast Guard is currently working on a regulatory project that would propose to revise the security training regulations for facility personnel to ensure all training is measured against a standard of competence, including the topics required under the SAFE Port Act. The Coast Guard is also working with the Maritime Administration to revise the existing model courses for facility personnel in order to meet the requirements in Section 109 of the MTSA and SAFE Port Act.

Question 14.: What steps has the Coast Guard taken to ensure that port workers are active participants in the Area Maritime Security Exercises?

Response: All of the Area Maritime Security Exercises include members of the Area Maritime Security Committee (AMSC), which typically include the security officers from private industry. These security officers participate in the planning of exercises, which increases awareness and participation, and take the lessons learned from the exercises back to educate their respective organizations. Additionally, the exercise sponsor sends out letters of invitation to the port community to further enhance participation.

Question 15.: Please provide us with information on the number of live port security exercises as opposed to tabletop port security exercises conducted every year.

Response: The table below outlines the number of live port security exercises as compared with tabletop port security exercises in recent fiscal years:

Fiscal Year	Tabletop	Live	Exercise Credit given for real world operation
FY 2005	34	18	0
FY 2006	44	13	4
FY 2007	37	8	3
TOTAL	115	39	7

*Notes: Tabletop category includes Tabletop and Functional (Command Post) exercises. Source of data is the Coast Guard's Congressional Biannual Report on Port Security Exercises.

Question 16.: Recently, the Department changed the way funds are distributed for Tier I and Tier II ports. While the Committee understands the interest in regional collaboration, explain why much of the financial oversight and paperwork requirements for distribution of these funds was moved from the Department to the fiduciary agent. **What are the advantages and disadvantages of a fiduciary agent for this program and will it continue in the future?**

Response: The oversight and paperwork requirements have not been moved from the Department to the Fiduciary Agent (FA). The oversight and paperwork requirements of the FA are the same as any grant award recipient. The difference is that the FA represents the interest of the entire port area, through the Area Maritime Security Committee, rather than an individual entity's interest.

In order to support strategic, regional port-wide risk management and business continuity planning processes and then have funds applied against the highest priority requirements based on the plan, the Department opted to award Port Security Grant Program funds to a FA to provide funding to a single point of contact for the grant award. The process allows for individual entities in a port area to cooperate with each other for funding rather than compete against each other.

The choice of the FA was left up to the Area Maritime Security Committee and had to be verified by the Coast Guard.

Question 17.: FEMA's guidance on grants is that they cannot benefit a federal agency. Many ports would like to share their camera feeds with Coast Guard. **Can ports share their information gained through equipment purchased through the Port Security Grant program with Coast Guard on an ongoing basis in order to promote interoperative communications? What limits are placed on this cooperation?**

Response: The guidance stipulates that "projects in which federal agencies are the primary beneficiary or that enhance federal property" are ineligible for award consideration. Another federal agency cannot be the recipient of another federal agency's grants, since this would be an augmentation of appropriations by the receiving agency. However, information sharing and interoperable communications are allowable with equipment purchased through the Port Security Grant Programs.

Question 18.: The largest port security costs to ports in the coming years relates to personnel costs and operation and maintenance of equipment, much of which was installed with the help of the Port Security Grant program. The Maritime Transportation Security Act allows grants to pay for operations and maintenance. **Will the Department allow for projects that relate to the operation and maintenance costs of already installed equipment? What are the limitations? What about replacement equipment?**

Response: The Port Security Grant Program guidance allows for limited operations and maintenance costs, specifically the cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers. In addition, routine maintenance costs for security monitoring, such as the cost of tapes for recording, are allowable. However, business operations and maintenance costs, such as personnel costs and items generally characterized as indirect or "overhead" costs, are unallowable.

(While personnel costs are allowable under MTSA, subsequent congressional actions—FY 2007 DHS Appropriations Act - have specifically excluded personnel costs as allowable.)

Question 19.: **Given the uncertainties of whether a man-made or natural disaster might strike next, what should be the current focus of efforts to ensure ports are prepared to respond and recover from a terrorist attack or natural disaster?**

Response: Ports should be preparing for both man-made and natural disasters. To prepare for both types of events the Port Security Grant Program has evolved from a program primarily focused on the security of individual facilities within ports, to a port-wide risk management/mitigation and continuity-of-operations/resumption-of-trade program that is fully integrated into the broader regional planning construct, which forms the core of the Urban Area Security Initiative, as well as applicable statewide initiatives.

Question 20.: The Department recently conducted TOPOFF IV in Portland, including some maritime venues. **What is being learned from recently conducted exercises at our ports, and how can one be sure these lessons are incorporated in planning and response efforts?**

Response: Results of the Coast Guard's Port Security Exercises have been reported to Congress biannually since October 2005. The latest report was signed and forwarded on July 26, 2007. The report outlines the following themes:

- The linkage and coordination of Area Maritime Security Plans (AMSP) to other relevant plans, along with updating plans with current information, continues to challenge efficient AMSPs implementation.
- The need for improved interoperable communications and situational awareness tools.
- Some lack of familiarity with the National Incident Management (NIMS)/ Incident Command System (ICS), AMSPs, and the associated roles and responsibilities of port partners.

In May 2006, the Coast Guard implemented the Remedial Action Management Program (RAMP) as a module in the Coast Guard Contingency Preparedness System (CPS). This program established procedures and processes for identifying, validating, assigning remediation responsibilities and monitoring the remediation of challenges identified during exercises. Additionally, results of the Biannual Port Security Report have been forwarded to the Coast Guard's AMSP program manager for review and consideration by its AMSP working group during AMSP revisions.

Question 21.: What has Coast Guard determined will be the impact of reducing the rotation length for facility inspectors, given the training and experience needed for effective facility oversight? What information was this assessment based on?

Response: The Coast Guard anticipates no impact from the change in rotation length. There are currently 389 qualified facility security inspectors in billets and more than 80 members with the qualification but not working in inspector positions who can be rotated into units as other members are rotated out. Additionally, the training for the facility security inspector qualification is being refined and will be provided to more members, further increasing the pool of qualified individuals to be rotated through the security inspector positions.

Question 22.: To what degree is the Coast Guard confident that resources would be available to handle heightened MARSEC level requirements if the level were raised for (a) a single sector, (b) several sectors, or (c) nationwide?

Response: The Coast Guard is confident that resources would be available to handle heightened MARSEC level requirements whether the level is raised for a single Sector, several Sectors, or nationwide. The Coast Guard's confidence is based on the combination of several measures and/or provisions that are already in place within the Operation Neptune Shield (ONS) Operations Order (OPORD), which promulgates Coast Guard-wide guidance and standards for conducting maritime security and response operations.

It is important to note that from the Coast Guard's planning perspective, only MARSEC 1 is expected to be sustained indefinitely. The Coast Guard has always envisioned that elevated MARSEC levels (2 and 3) would be sustained for relatively short periods of time (the specific sustainment requirements contained in the ONS OPORD are classified), and that MARSEC 3 would be focused on one or a few specific Sectors or geographic areas (MARSEC 3 is set only when an attack is deemed imminent or has already occurred).

In responding to a maritime security threat, the Coast Guard employs threat-based, risk-managed principles, matching protective/preventative efforts to the threat's nature (i.e., attack method, target, etc.). By using these principles, the Coast Guard implements MARSEC level increases that are focused on a single or few Sectors or, if nationwide, only on the targeted type of maritime critical infrastructure and key resources (e.g., maritime mass transit—ferries or vessels carrying Certain Dangerous Cargoes). The Coast Guard leverages the support of other government agencies and ensures that maritime industry stakeholders have increased their security efforts in accordance with their Coast Guard-approved facility and vessel security plans. Coast Guard Sector Commanders carrying out the operational security measures dictated by increased MARSEC levels may request additional resources, i.e., deployable specialized forces, from the Deployable Operations Group via their Area Commander. Boarding teams, vessel escort assets, and other resources may be dispatched from Maritime Safety and Security Teams or at the high end level from the Maritime Security Response Team. Finally, when MARSEC 2 or 3 is imposed, the ONS OPORD pre-authorizes Area Commanders to temporarily adjust the level of effort in other Coast Guard missions, as necessary in order to make additional resources available to the Ports, Waterways, and Coastal Security missions.

Question 23.: With the supplemental funding to the USCG providing for additional facility inspectors, will the USCG have enough fully trained and experienced inspectors for effective facility oversight?

Response: Yes, the Coast Guard has sufficient personnel with the necessary qualifications to exercise effective oversight of the regulated facilities in the United States. We currently have 389 facility security inspectors in place to meet the compliance check requirements with an approximately 80 more to rotate into those billets as others rotate out. During calendar year 2007, the complement of facility security inspectors performed in excess of 9,000 compliance checks, including both annual inspections and spot checks, of our approximately 3,200 regulated maritime facilities.

Question 24.: Given available resources, to what extent will Coast Guard perform 2 inspections (at least 1 unannounced) at each MTSA-regulated facility? If resources do not allow CG to perform unannounced inspections at all facilities, how will CG determine which facilities to inspect?

Response: The Coast Guard currently has 389 facility security inspectors in place and has performed in excess of 9,000 facility inspections, both announced annual exams and unannounced spot checks, of our 3,200 regulated facilities during calendar year 2007. As such, there has been no need to make determinations of which maritime facilities to leave out of the inspection cycle.

Question 25.: Based on one announced annual exam and one unannounced spot check, how confident is the US Coast Guard that MTSA-regulated facilities are maintaining compliance with MTSA?

What are Coast Guard facility inspectors finding during facility inspections?

Are Coast Guard facility inspectors finding greater non-compliance during unannounced vs. announced inspections? If so, why aren't all inspections unannounced?

Response: The Coast Guard is confident that U.S. maritime facilities are maintaining substantial compliance with the regulations and their approved Facility Security Plans based on one announced annual exam and one unannounced spot check each year.

Inspectors are finding the majority of non-compliance issues center on access control, monitoring, and training of facility personnel. In general, these tend to be easily corrected.

The Coast Guard finds more instances of non-compliance through the announced annual exam than through unannounced spot checks. The reason being the annual exam is much more thorough, covering all facets of the Facility Security Plan, and provides greater opportunity to closely review records, etc. The unannounced spot check, while useful, is more limited in scope and intensity.

Question 26.: When is the Coast Guard going to finalize the International Seafarer Identification regulation? This regulation was originally required five years ago and I do not understand why it has taken so long for the Department to complete it.

Response: Prior to the enactment of the SAFE Port Act of 2006, Coast Guard action on the rulemaking project to implement crewmember ID requirements of 46 USC 70111(a)(b) was suspended awaiting the results of the Tripartite Advisory Panel on International Labor Standards (TAPILS) consideration of the International Labor Organization section 110 of the SAFE Port Act independently of whether the United States Government ratification "Seafarers Identify Document Convention" (ILO 185) as well as a decision on whether the United States Government would ratify the Convention. The Coast Guard is now proceeding with a rulemaking titled "Crewmember Identification Documents" to fulfill the requirements of section 110 of the SAFE Port Act independently of whether the United States Government ultimately ratifies ILO 185, and will complete it as expeditiously as possible.

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE
ON HOMELAND SECURITY

RESPONSES FROM THOMAS WINKOWSKI

Question 1.: One of the primary goals of the Safe Port Act is the improvement of risk targeting for maritime cargo containers inbound to U.S. ports from overseas locations. Sec 203 of the Act provides the authority for enhancing data for risk targeting to provide this layer of security to address the maritime cargo security vulnerability that we continue to face as a Nation. I understand that the Department is has been developing an initiative for the past year known as 10+2 which will meet this requirement.

**What is the status of the initiative?
When is it going to be finalized?**

Why has it taken over a year to develop?

Response: The Security Filing (10+2) Notice of Proposed Rule Making (NPRM) was published in the Federal Register on January 2, 2008, at 73 FR 90. The 60-day public comment period for the proposed rule ends on March 3, 2008. During this comment period, any and all interested parties are invited to submit comments on the proposal. CBP will consider all comments received during the comment period in development of the Final Rule. The Final Rule is subject to review by the Office of Management and Budget and must be approved by the Secretary, DHS.

CBP worked in close concert with the trade community, and the Commercial Operations Advisory Committee (COAC) in particular, to develop the current targeting enhancement proposal known as the "10+2" initiative. While preliminary discussions had been ongoing prior to enactment of the SAFE Port Act in October 2006, CBP commenced its formal discussions with COAC in November 2006, and completed the consultation process in February 2007. This joint effort produced over 30 recommendations for consideration as it refined the initial "10+2" proposal that forms the basis for the draft Notice of Proposed Rule-Making (NPRM).

The ability of CBP and the trade community to produce such an important proposal in a short time is a tribute to the cooperative relationship between the agency and its stakeholders. It is especially remarkable, given the complexity of the issues under consideration and the variety of interests (carriers, customs brokers, freight forwarders, and importers) represented.

Question 2: I also understand that the Department has developed a Global Trade Exchange (GTX) initiative to provide deeper risk assessment on containers for importers who volunteer to share data on inbound maritime cargo containers.

What is the status of GTX?

What role has industry played in developing this new initiative? It's my understanding that Department has deliberately limited industry input and that industry representatives do not support it.

Response: On December 11, 2007, CBP issued a Request for Quotation (RFQ) soliciting bid proposals from the vendor/contractor community for the development and implementation of the Global Trade Exchange (GTX). Specifically, the RFQ outlined the requirements for the development of a privately operated, self-sustaining trade information system that will collect commercial transaction data not currently available to CBP from parties in the supply chain who have contracted or provided services for the of international shipments. The system, furthermore, will allow government and trade community participants to input and access trade data through an information broker. When combined with existing CBP tools, GTX will allow CBP to identify and target suspect shipments/transactions well in advance of a shipment's entry into a supply chain.

Vendor proposals (due by January 22, 2008) have been received by CBP and are currently under review by a Technical Evaluation Working Group. The review process will be completed within the next 30 to 45 days. Advancement of GTX will be based on the review results and recommendations produced by the Technical Evaluation Working Group.

It is important to note that the issuance of the is the first step in a process that will culminate in the implementation of a GTX pilot program specifically designed to test the GTX concept, establish requirements, and identify issues. Therefore, we believe that GTX should be viewed as a developmental process through which CBP, private sector vendors, and the trade community will develop an advanced, forward-thinking cargo data warehouse.

Question 3: How has CBP fostered cooperation with international organizations and foreign governments to maximize the benefit of the CSI program?

How has CBP worked with international organizations and foreign governments implementing CSI related initiatives regarding global security standards and practices to improve maritime and container security?

Response: CBP has utilized the CSI annual Global Targeting Conference and the activity of the World Customs Organization's Framework of Standards to maximize the benefits of the CSI Program.

The annual CSI Global Targeting Conference held in Washington, DC, sponsored by CBP, brings together several hundred customs representatives from over 30 countries that participate in the CSI program to discuss "best practices" and the development of significant security protocols used in their respective countries and the deployment of large scale imaging devices. For, this year's conference, which was held in August 2007, CBP hosted 200 foreign customs and embassy officials as well as officials the Department of Energy, Department of State and Department of Homeland Security (including United States Coast Guard, CBP Representatives and

Immigration and Customs Enforcement stationed in over 25 countries). During the conference, CBP Senior officials met with 34 Directors Delegates to discuss key issues and program concerns and identify opportunities for continued improvement.

Because of these two forums, the utilization and capacity of non-intrusive inspection (NII) equipment has increased globally.

CBP's Office of International Affairs and Trade Relations (INATR) has taken a leading role in improving cargo security through the creation of the World Customs Organization (WCO) SAFE Framework of Standards. Guided by the SAFE Framework, CBP works with foreign governments to improve risk management procedures, increase use of intrusive inspection (NII) equipment, and encourage countries to exchange advance electronic information. This international cooperation ensures the security of cargo at every link in the supply chain, the SAFE Framework supports the CSI program. Related work has also been carried out with other international organizations such as the International Maritime Organization (IMO), the International Organization on Standardization (ISO) and the Organization for Security and Co-operation in Europe (OSCE).

Through CBP's Capacity Building Branch within INATR, CBP is providing training and technical assistance to the customs administrations of a number of countries that currently participate in CSI, including Brazil, Honduras, the Dominican Republic, and South Africa. This training and technical assistance forms a long-term capacity building program to support implementation of the World Customs Organization Framework of Standards to Secure and Facilitate Global Trade. The standards incorporated in the Framework incorporate many of the key elements that support CSI, including: the advance electronic presentation of cargo information; the screening of cargo containers using non-intrusive inspection equipment; the use of automated risk management systems; the standardization of targeting criteria to identify high-risk cargo and containers; an emphasis on employee integrity programs; and the inspection of cargo in the country of origin, transit and destination.

CBP's Training and Assistance Division of INATR currently provides a number of assistance and training programs to foreign customs and border security agencies to facilitate implementation of port security antiterrorism measures. Through its Capacity Building program in support of the World Customs Organization Framework of Standards to Secure and Facilitate Global Trade, CBP provides a long-term training and technical assistance program to partner with customs administrations that includes an depth assessment of its seaport security practices.

Question 4.: How does CBP ensure that the number of staff located at CSI ports is appropriate and how has it systematically looked for efficiencies that may result from moving targeting operations to the U.S. so that resources are not kept at CSI seaports in perpetuity?

Response: As part of CBP's evaluation process, CBP conducts annual evaluations of its CSI ports, concentrating in part on workload increases or decreases. CBP uses these findings to adjust resources at the U.S. National Targeting Center, Cargo (NTCC) and at overseas CSI ports, as appropriate.

CBP has also reviewed General Accountability Office (GAO) reports that have identified shortages in human resources at some CSI ports and have agreed with and implemented the recommendation to augment CBP personnel at the NTCC to perform remote targeting for CSI in high volume ports.

CBP will also use "lessons learned" from the Secure Freight Initiative (SFI) to determine the feasibility of remote targeting from the NTCC. CBP is considering technological solutions to possibly reduce CSI human resources deployed abroad while still ensuring that containers destined for the U.S. are examined for weapons of mass destruction.

Question 5.: How does CBP ensure that all high risk containers identified at CSI seaports are inspected and that the inspections processes and equipment are sound and used effectively?

Response: Host government officials have provided CBP with all relevant information about the equipment used for the inspection of containers. Based on this information, CBP has determined that the equipment used by host governments at CSI seaports is equal to or in some instances, more technologically advanced than the equipment used by CBP at its domestic ports. CBP officers are fully trained in the equipment being used by the host government and in the cases where CBP has provided NII equipment to the host government, the host government customs officers have been trained in the use of that equipment.

Since its inception more than six years ago, the success of the CSI program can be attributed largely to the cooperation and collaboration the program fosters between the U.S. and its host government counterparts in examining high-risk containers that are referred to host government for inspection. To date, there has been

no Weapon of Mass Destruction detected at a CSI port or on U.S. destined containers once they arrive in the U.S. CBP reexamines containers in the U.S. a result of its own Compliance Measurement program and sometimes as the result of policies that the local port authorities establish.

Question 6.: How has CBP ensured that the seaports that it has selected for the CSI program—those receiving staff, equipment, and other U.S. resources—provide the greatest benefit for the program, and what are plans for managing future program participation, including how ports may be phased out of the program and others brought in?

Response: CBP conducts yearly evaluations of its CSI ports and, as part of that evaluation process, reviews the workload and whether it has increased or decreased. The evaluation process also examines the CSI team's interaction with the host government counterparts and how that relationship is working. Since the CSI program is essentially a partnership between the U.S. and the host government, effective communication is very important to its success. With each evaluation of a CSI port, CBP will continue to use these CSI port evaluations and the increase in port efficiency in jointly targeting high-risk containers with host government counterparts to determine if any shift of resources to either the NTCC or another CSI port needing additional resources, is required. For those CSI ports that were provided with loaner NII equipment, CBP receives daily reports on usage of the NII equipment and the usage and downtime is tracked on a daily basis.

Question 7.: Should CSI be expanded beyond the 58 ports currently planned for the program? If so, to what extent is planning underway to account for this, such as redeployment of staff to additional ports?

Response: The focus is currently on determining the feasibility of 100% scanning required by the SAFE Port Act. Therefore, CBP is holding off on future expansion of CSI until after the agency reports to Congress in April on the feasibility of 100% scanning based on the results of the Secured Freight Initiative (SFI) pilot.

However, it should be noted that CSI was never intended to cover 100% of maritime cargo destined to the U.S. CBP relies on a risk management approach with a continued focus on identifying and inspecting 100 percent of those shipments that have been designated as high-risk, and increasing DHS' ability to scan cargo for the presence of nuclear or radiological material. CBP's goal is to continue to inspect 100 percent of all high-risk shipments. As part of this risk management strategy, CBP uses a multi-layered approach to ensure the integrity of the supply chain from the point of stuffing through arrival at a U.S. port of entry. CBP's multi-layered defense includes:

- 24-Hour Rule: Under this requirement, manifest information must be provided to CBP 24 hours prior to a U.S. destined sea container being loaded onto a vessel at a foreign port.
- Screening and Inspection: CBP screens 100 percent of all cargo before it arrives in the U.S. using intelligence and cutting edge technologies, and inspects all high-risk cargo. CBP may deny the loading of high-risk cargo while the vessel is still overseas.
- CSI: Enables CBP, in working with host government customs services, to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the U.S. CSI ports are operational in 58 ports covering 86 percent of maritime containerized cargo shipped to the U.S.
- C-TPAT (Customs Trade Partnership Against Terrorism): CBP created a public-private and international partnership businesses know as the Trade Partnership Against Terrorism (C-TPAT),” that includes most of the largest U.S. importers. Through C-TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security.

Question 8.: According to GAO, CBP faces difficulties in recruiting qualified staff for CSI and in some instances has deployed personnel overseas without the requisite training. How does the agency plan to address these challenges?

Response: As with any expanding program, CBP has had challenges in recruiting staff for CSI. However, CBP has followed recommendation lead is in addressing these challenges by moving some of the targeting duties to NTCC and establishing minimum staffing levels at hard to fill ports, thus not impacting CSI operations of screening and targeting high-risk shipments for terrorism. CBP Officers that did not receive the requisite formalized training prior to being deployed were placed in a location that had a highly experienced officer that provided on-the-job training. This lack of formalized training did not have a negative impact on port operations as reported by the CSID team that conducted the port evaluation. It should be noted that

once the office was fully staffed, those individuals were returned for formalized training.

Question 9.: Legal restrictions in several host countries bar CSI teams from viewing examinations conducted by host customs authorities and these containers are rarely re-examined upon arrival in the U.S. **Does it make sense to have CSI teams in such countries when we do not participate in the inspections?**

Response: Of the 32 countries where CSI is operational, there is only one country that does not allow CBP personnel inside the x-ray examination vehicle. However, this country provides CBP with a copy of the x-ray image and, together with the information obtained through our own targeting analysis and information provided our host government counterpart, we are able to make a sound determination of whether a container poses a risk for terrorism. What is important here is that face-to-face communication goes very far. By having CBP Officers stationed in-country, we are able to build and establish clear communication channels that were not in existence prior to this initiative. CBP has placed experienced officers that have been trained in targeting analysis and image interpretation. If these officers are not comfortable with the examination process, there are protocols in place. The CBP Officer can request a "hold" for domestic examination or call the NTCC to issue a "Do Not Load" order.

CSI is now operational in 58 foreign seaports covering approximately 86% of maritime containerized cargo destined to the U.S. The success of this program is attributed to the cooperation and collaboration of our foreign partners. To date, there have been no Weapons of Mass Destruction detected at the CSI ports or on containers that have been reexamined when arriving in the U.S. because of own Compliance Measurement program and local port policies.

Question 10.: Although recommended by GAO and the SAFE Port Act, minimum technical operating standards for non-intrusive inspection equipment at CSI ports have yet to be established. **Without such standards, what assurances does our nation have that this equipment is capable of detecting weapons of mass destruction within high-risk containers?**

Response: CBP has taken steps of achieving uniform standards through the World Customs Organization (WCO). The CSI program has been in operation for over five years, and can attribute its largely to the cooperation and collaboration that the program fosters between the U.S. and its host government counterparts in examining high-risk containers that the U.S. refers to the host government for inspection. To date, there has been no Weapon of Mass Destruction detected at a CSI port or on containers that have been reexamined when arriving in the U.S. Reexamination occurs at a U.S. port due to own Compliance Measurement program and as a result of local port policies. Additionally, CBP the installation of Non-Intrusive Inspection equipment in 13 CSI ports; all such equipment meets the established standard for U.S. deployed NII in at domestic ports.

Recognizing that a nation's sovereignty is critical and that CBP is not a standard setting agency, we will continue to work with the World Customs Organization (WCO) through its Safe Framework of Standards to address a uniform customs process and technical standards for equipment to ensure that the examination process of cargo and equipment used as part of the process is one that is uniform throughout the world.

Question 11.: CSI has entered into an arrangement with New Zealand whereby containers bound for the U.S. are scanned and the resultant images beamed directly to National Targeting Center for review. **Does this system constitute a model that could be expanded to other countries?**

Response: The New Zealand project is unique in many ways. The similarity with CSI partners is that New Zealand must meet the requirements established under CSI. The uniqueness is that like the U.S., New Zealand has a national targeting center with 24x7 operations. New Zealand also has a 48-hour rule (the U.S. has a 24-hour rule) that requires shippers to provide all of the data requested by CBP. New Zealand is also a trusted partner and the majority of the shipments arriving into the U.S. are low-risk for terrorism. Moreover, New Zealand has similar NII equipment which, through the use of special software, allows CBP Officers at the NTCC to manipulate the image. This software can only interpret Smiths HCV units. Along with the software, there is a special key (aka dongles) which allows only certain workstations to view the images. We currently have 3 workstations at the NTCC with these special keys.

Also crucial to this operation is that New Zealand the limited amount of time (20 minutes) that each country has to respond to the other's request to determine the potential risk of a shipment. This is a mutually agreed upon time limit that was

established with the objective of ensuring the expeditious movement of low risk cargo through the international supply chain.

This pilot program did not come without challenges. As the file size of the images average about 11MB, which is too large for any CBP mail account (images were previously sent via the Office of Information Technology (OIT) had to create a special mailbox that is capable of receiving files of this size.

CBP has also tried to test the same concept with another trusted partner with shipments that are low-risk to terrorism. Unlike New Zealand the other trusted partner being considered does not have a national targeting center, has no 24 or 48-hour rule and, does not have NII equipment that will allow the NTCC to manipulate the x-ray image. For this particular NII equipment, CBP is unable to obtain a license for the special software that is required to view and manipulate the x-ray image. Also, the other trusted partner's customs service has had difficulty providing timely information on specific containers, which has resulted in required information being delayed for 16 hours. With such a delay, often times a container of interest would have already been laden upon the vessel and unavailable for examination.

Question 12.: Provisions in Sec 216 of the SAFE Port Act call for benefits to participants in the C-TPAT program who demonstrate a sustained commitment to cargo container security. Among the criteria for Tier 3 C-TPAT recognition is submission of additional cargo information prior to loading of the container. **What does CBP plan to do to more fully define the incentives that would encourage private sector provision of this data that in turn would permit more targeted and accurate risk assessment of inbound cargo containers?**

What's the status of additional benefits for C-TPAT members, especially Tier III participants?

Response: The C-TPAT program continues to evolve with respect to providing facilitation benefits to importer partners in return for proof of strong supply chains. C-TPAT believes that the current Tiered benefit structure that includes Tier 3 and the criteria determine such benefits provides importer partners with appropriate benefits for their level of supply chain security.

As part of its layered enforcement strategy, CBP requires the submission of advanced manifest data for purposes of targeting high risk shipments. The trade benefits from the submission of advanced data in that, if entries are filed timely, the goods can be cleared in advance of arrival as well as allow for more efficient shipping and inventory data.

C-TPAT will continue to examine the Tier benefit structure in an effort to ensure that the program is addressing the needs of its current and future membership as well as the needs of CBP.

As of December 14, 2007, 232 C-TPAT importer partners were receiving TIER benefits.

Question 13.: How does CBP assess effectiveness—in terms of outcome-based performance measures—and that the tax resources expended are providing the level of security promised by the program?

Response: C-TPAT has updated its five-year strategic plan and developed several performance indicators, which will be used to measure the effectiveness of the program. For example, C-TPAT measures program performance based on SAFE Port Act mandated goals such as reviewing newly submitted security profiles within 90 days, ensuring that initial validations occur within 1 year, and that revalidations occur within 3 years.

The program also measures its success against internal goals such as completing a specific number of validations and revalidations each year, as defined by the C-TPAT annual plan. The C-TPAT program also ensures that all expenditures, including travel, equipment, and salaries are properly monitored by supervision and adhere to normal budgetary controls.

The success of the C-TPAT program was validated by recent a study conducted on behalf of CBP by the University of Virginia. More than 1,700 member companies chose to participate, with over half being U.S. importers and some of the nation's largest retailers. The study demonstrates the effectiveness of C-TPAT in causing thousands of companies to give closer scrutiny to the security of the goods they handle and ensuring that their overseas suppliers have implemented sound security practices. C-TPAT will undertake future studies of this sort to continue to assess the program's effectiveness.

Question 14.: After initial validation of the security measures in member companies' security profiles, how are security changes monitored and validated for continued adherence to C-TPAT security requirements?

Response: C-TPAT utilizes a variety of strategies to monitor compliance with the program. As mandated by the SAFE Port Act, all C-TPAT participants must be re-validated within 3 years of their original validation. Due to risk, the C-TPAT program has determined that it is prudent to validate all Mexican Highway Carriers on an annual basis. C-TPAT constantly reviews CBP seizure reports and where a member is involved in a security breach, C-TPAT immediately undertakes a Post Incident Analysis to determine if there was a systemic breakdown in the member's security procedures. Finally, all C-TPAT participants are required to conduct an annual self-assessment in which the member is asked to review, correct update its previously submitted security profile.

Question 15.: What did it cost to develop the Validation Security Assessment Tool (VSAT), how is CBP using the VSAT in performing foreign supply chain validations, and what benefit is the C-TPAT program deriving from using VSAT? What reviews and analysis of VSAT is done by CBP supervisors and management to ensure it is being used right and producing results?

Response: The final cost to develop the Validation Security Assessment Tool (VSAT) was included within the original C-TPAT IT operational budget and the specific cost is therefore estimated at around \$5,000 USD.

The Supply Chain Security Specialists (SCSS) are required to use the VSAT tool as part of the validation visits. The VSAT ensures that validations are uniform by using standard questions. The use of the VSAT does not preclude the SCSS from asking additional questions during the course of a validation, which allows the SCSS to get a complete and detailed snap shot of a company's overall supply chain security. Field Office Supervisors are required to perform random, quarterly audits of the VSAT data collected by SCSS to ensure information is complete, timely, and accurate.

C-TPAT will consider ways to systematically analyze VSAT data moving forward.

Question 16.: What other steps, if any, has CBP taken to reduce the risks that C-TPAT shipments that originate in or move through high risk countries will be tampered with on their journey to the U.S.? How would we even detect such tampering today? Are Tier 3 shipments from countries subject to a higher inspection rate than other Tier 3 shipments? How much higher? Is that rate adequate to offset the risk of tampering en route?

Response: CBP will continue to target and examine shipments based on risk. Shipments unknown or less established entities, and from higher risk countries, receive higher scrutiny from CBP. C-TPAT recognizes the complexity of international supply chains and requires C-TPAT members to implement security measures based upon risk. C-TPAT membership is one of several factors taken into account by CBP when determining which shipments will be referred for security inspection.

C-TPAT's minimum security criteria require that all C-TPAT partners conduct business with enterprises that comply with that criteria resulting in less potential for tampering. C-TPAT importer partners commit to strengthen their entire supply chains and adopt appropriate security measures based on risk, and cannot exclude a particular segment of their supply chain from this commitment. Importers must ensure business partners develop security processes and procedures consistent with the CTPAT criteria to enhance the integrity of the shipment at point of origin, and throughout the supply chain. C-TPAT members periodically review their business partners' processes and facilities.

One of the requirements for C-TPAT importers and sea carriers is that all containerized cargo must have a high security seal affixed to all loaded containers bound for the U.S. All seals used or distributed by the sea carrier must meet or exceed the current PAS 17712 standards for high security seals, and the seal number must be on all shipping documents.

Question 17.: In the past, GAO has identified weaknesses C-TPAT's in validation process. What efforts has CBP made to correct these deficiencies? Is the current validation process rigorous enough to meet the intended purpose to ensure that companies are actually implementing their supply chain security plans?

Response: C-TPAT has undertaken a pro-active approach to address potential weaknesses in the validation process that may have occurred since first implementation, by ensuring that the validation process is as complete and as rigorous as possible.

1. As mandated by the SAFE Port Act, all C-TPAT participants must be re-validated within 3 years of their original validation. Due to risk, the C-TPAT program has determined that it is prudent to validate all Mexican Highway Carriers

riers on an annual basis. Revalidations ensure companies are continuing to assess their supply chain and addressing changing risk factors.

2. The Validation Security Assessment Tool (VSAT) was specifically designed to ensure uniformity in the validation process. The VSAT is required to be used by all SCSS that perform a foreign validation visit. The VSAT ensures that validations are uniform by using standard questions; critical security related questions are asked by all SCSS. The use of the VSAT does not preclude the SCSS from asking additional questions during the course of a validation, which allows the SCSS to get a complete and detailed snap shot of a company's overall supply chain security. Field Office Supervisors are required to perform random, quarterly audits of the VSAT data collected by SCSS to ensure information is complete, timely, and accurate.

3. Each SCSS receives initial training on the validation process. In addition, C-TPAT conducts semi-annual training for all SCSS and includes updated information on the validation process.

4. In ensuring its continued viability, effectiveness, and relevance, the C-TPAT program continues to evolve as the terrorist threat and the nature of global trade evolves. C-TPAT implemented new security criteria to most trade sectors to ensure companies are compliant with minimum security standards. The impetus for strengthening security "guidelines" into security "criteria" was to provide more detail to C-TPAT members regarding the expectations of the program. The new security criteria were also issued to assist CBP in defining a more consistent baseline for minimal program requirements and better-defined TPAT benefits.

All validation reports outline the manner in which the validated company is meeting the criteria, or failing to do so. C-TPAT companies that fail to adhere to the C-TPAT standards, as defined by the minimum security criteria, are either suspended or removed from the program.

5. C-TPAT recently issued a new Memorandum of Understanding (MOU) for all members. The new MOU addresses the validation process to ensure greater uniformity throughout all validations.

6. C-TPAT participants are reminded that part of their program membership includes the need to perform an annual self-assessment. Participants are asked to review, correct update their previously submitted security profile. Failure to do so results in suspension or removal from the program.

Question 18.: Despite the huge volume of Chinese imports entering the U.S. everyday, the Chinese government does not permit CBP to perform validations within its borders. **How does the agency plan to adapt the C-TPAT program to capture this vital section of the supply chain?**

Response: Congress, through the SAFE Port Act, required C-TPAT to develop a third party validation pilot program to assess the feasibility of having non-government entities conduct validations on behalf of the program. As a result of this congressional mandate, CBP implemented a pilot program to use third parties to validate C-TPAT members operating in China. The Commercial Operations Advisory Committee officially approved the plan in February of 2007.

C-TPAT identified 304 importer partners that have 75 percent or more of their supply chain in China and which are in Tier 1 status (certified), and invited each individually to participate in this pilot program. To date, 14 certified importer partners have elected to participate in the pilot. A third party China validation visit was completed in late November. At the conclusion of the pilot on May 1, 2008, C-TPAT will prepare a report to Congress, which will include lessons learned.

In an effort to allow SCSS to conduct validations in China, CBP and the Government of China (GOC) are currently developing a statement of cooperation regarding a joint validation pilot. A joint validation project is tentatively scheduled for March 10—21, 2008.

Question 19.: **Why has CBP not developed the container security device required by the SAFE Port Act?** I have been briefed by numerous vendors and I know that the technology exists.

What technology has CBP tested to validate its assertion that the technology does not exist?

Response: On December 12, 2007, CBP published A "Request For Information, (RFI) Regarding Conveyance Security Devices" on the FedBizOppa website. The announcement will be open for a sixty day period (from December 12, 2007 to February 8, 2008). The goal of this RFI is to identify currently available Conveyance Security Device (CSD) Systems. Once and CSD systems are provided to CBP by the vendor, they will be tested to determine whether the technology meets the minimum tech-

nical requirements outlined in the RFI. The testing will first be conducted in the laboratory, followed by operational testing.

Question 20.: The SAFE Port Act called on the Department to conduct a one-year pilot program to assess the risk posed by, and improve the security of, empty containers at U.S. seaports. This pilot has not yet begun. When are you planning on starting it?

Response: The 12-month empty sea container pilot program will commence on February 1, 2008 and continue through January 31, 2009.

Question 21.: According to Philip Spayd in an August 27, 2007 article in the Journal of Commerce regarding the Recovery Plan mandated in the SAFE Port Act: "many in the trade community anticipated an operational plan that would clearly set out the roles and responsibilities of government officials who would manage a trade security incident. What they received was a 128-page plan that would receive a high grade as a research project for a graduate school class in international logistics, but which lacks any operational grounding." What is your response to this critique?

Response: The 128-page report referenced by Mr. Spayd is the *Strategy to Enhance International Supply Chain Security* (July 2007)—a strategic document. Operational planning is ongoing between CBP and the U.S. Coast Guard (USCG) to publish the *CBP/USCG Joint Protocols for the Expeditious Recovery of Trade (Recovery Protocols)*. This operational-level document would memorialize CBP and USCG roles and responsibilities for communicating and coordinating with government agencies and the trade community during a Maritime Transportation Security Incident. The Recovery Protocols is currently undergoing final review within both agencies. As part of the Recovery Protocols, two advisory groups will be formed with members of industry, the Carrier Support Group and the Trade Support Group, to ensure close coordination occurs on all trade recovery efforts.

Question 22.: Section 201 of the SAFE Port Act required a Strategic Plan to Enhance the Security of the International Supply Chain. This plan was supposed to include protocols for the expeditious resumption of the flow of trade in the event of a transportation disruption or a transportation security incident. According to GAO, the Department did not achieve success with this plan. Secretary admitted this fact at an August 16, 2007 meeting of the Advisory Committee on Commercial Operations for U.S. Customs and Border Protection. He told COAC members that day that the final product "not a detailed plan."

When is the Department going to produce a detailed plan?

How much money did the Department spend on this less-than-successful document?

Response: The Strategic Plan provides overarching protocols for the prioritization of vessels and cargo, identifies incident management practices specific to trade resumption in support of the National Response Framework, and describes guidance for the redeployment of government resources and personnel. In doing so, the strategy recognizes that there exist many different types of incidents which might impact the supply chain, but that resumption itself is an "all hazards" requirement.

The USCG and CBP are part of a joint Senior Guidance Team that is developing both tactical protocols for communications with the trade, and agency-specific plans for resumption activities. Further, in keeping with the Maritime Transportation and Security Act of 2002 (MTSA), the Area Maritime Security Committees are in the process of developing resumption annexes to each of the Area Maritime Security Plans. These revisions to the area plans are being conducted within the timelines of the mandated review and update cycle, with completion scheduled for mid-2009.

The Department expenses associated with this plan were principally in the area of staff resources. A writing team of approximately 30 individuals from across the components and agencies worked on the document over the 270 days of its development. Some individuals contributed greater amounts of time, depending upon their organizational involvement in the subject matter. At the Department headquarters level, the project lead, who conducted the majority of the review, consolidation, and drafting work, was a U. S. Coast Guard 0—5 detailee. An estimated 40% of his time over the development cycle was devoted to the project.

Question 23.: It's my understanding the Customs and Border Protection advised the countries on what technology to purchase. How did CBP determine which technology to use?

Response: CBP partners with the Department of Energy (DOE) to provide and procure the scanning equipment in most of the ports. DOE, through its Megaports Initiative, contributes the radiation detection equipment, optical character recogni-

tion (OCR) technology, and the communications system, as well as training and maintenance while CBP is responsible for the Non-Intrusive Imaging (NII) equipment. Both DOE and CBP work with host governments and terminal operators to ensure that the best available equipment is used to scan containers for radiation and capture images for analysis. Many factors affect what technology will be used including container volume, port operations, physical characteristics of the port, among other factors.

Question 24.: CBP is currently testing advanced spectroscopic portals in New York. The testing on this testing won't be completed for several months. Despite this fact, the Department of Energy decided to purchase 12 of the portals—several of which will be placed in Southampton, England, one of the ports. **Why did the US government purchase equipment that has not yet been vetted—isn't this a waste of money?**

Response: DOE is confident that Advanced Spectroscopic Portal (ASP) monitors will work effectively as a secondary inspection tool. DOE is currently evaluating an ASP at the Port of Southampton in the United Kingdom to help better define the most effective operational scenarios for secondary inspection. DOE will conduct additional operational evaluations at the Los Alamos National Laboratory in early 2008. At this time, DOE has no plans to deploy as a primary inspection tool, and has made no commitment to purchase any more units at this time.

DOE believes that the ASP will improve secondary inspections for several reasons. First, the ASP is essentially a larger, stationary version of the handheld Radioactive Isotope Identification Device (RIID) currently used for secondary inspections. In contrast to the RIID, whose effectiveness is *affected* by the motivation and training of the user, the ASP makes the same scan every time. Second, the ASP detector array surrounds the cargo container, allowing it to view a radioactive source from multiple angles. The larger detector area also achieves statistical accuracy in the spectrum more quickly. Finally, the ASP uses air conditioning for temperature stabilization. The "gain" of Sodium Iodine instruments, which is important to accurate identification, is temperature dependent. In contrast, the handheld RIID must be recalibrated when the temperature changes.

Question 25.: The SAFE Port Act required CBP develop an evaluation plan to assess the results of the pilot program. **What factors should be considered in this evaluation plan?**

Response: The SAFE Port Act requires the Department of Homeland Security (DHS), in conjunction with the Departments of Energy (DOE) and State (DOS), to submit a report to Congress six months after the first three pilot ports became fully operational. Southampton, United Kingdom; Qasim, Pakistan; and Cortes, Honduras, became operational on October 12, 2007. In April 2008, DHS will submit a report to Congress on the lessons in these three ports as well as four additional, limited capacity ports: Korea, Hong Kong, Singapore, and Salalah, Oman. As data for the report is collected, the metrics for evaluation continues to be refined. Some examples of factors to be considered are: the effect on port operations; the reliability and performance of the equipment; and lessons learned during the negotiations with host governments.

PANEL II

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON
HOMELAND SECURITY

RESPONSES FROM MARY K. ALEXANDER



January 3, 2008

The Honorable Bennie G. Thompson
Chairman, Homeland Security Committee
U.S. House of Representatives
Washington, DC 20515-6480

Dear Chairman Thompson:

Thank you for granting me the opportunity to testify at the October 30, 2007 hearing on the "SAFE Port Act: Status of Implementation One Year Later." I appreciated the chance to provide the views of the Joint Industry Group (JIG), and I am happy to answer the follow-up questions you have posed. For ease of reference, the responses offered from JIG are listed directly after each of the questions asked below.

Cargo Security

1. *It is my understanding that the Department has been developing the 10+2 initiative for over a year. What has the Department told you about when it is going to be finalized?*

Response: The JIG membership was never given a specific date regarding publication of the "10+2" notice of proposed rulemaking (NPRM), but we were told DHS hoped to release it by the end of the year. The NPRM was finally published in the January 2, 2008 Federal Register. Industry has until March 3, 2008 to file comments. We do not know how long it will take DHS to finalize the rule after all of the comments are received.

2. According to your written testimony, the Department has developed GTX behind closed doors. **Why do you think they have limited industry input?**

Response: We simply do not know why industry input was so limited during the development of the RFQ for the Global Trade Exchange (GTX) initiative. DHS was extremely inclusive during the development of the "10+2" initiative, and the trade community repeatedly expressed our gratitude for this collaboration. We do not understand why a similar course was not followed for GTX.

3. Please provide us with information about the concerns you have with the GTX initiative.

Response: Please see Attachment 1, which lists some of our primary concerns about GTX. These are comments we submitted to the Department of Homeland Security in August, and yet none of those issues were addressed prior to release of the RFQ.

Customs-Trade Partnership Against Terrorism

4. What, if any, difference in inspection levels have JIG members experienced as a result of C-TPAT enrollment?

Response: JIG members have slightly different viewpoints on the inspection levels they have experienced as a result of C-TPAT enrollment. Panasonic, for instance, has seen slightly fewer inspections with C-TPAT enrollment, but as a "low risk" customer, exam rates were low before September 11, 2001. As a group, however, our members have not reported significant decreases in inspection levels as a result of participating in C-TPAT. The only other tangible benefit has been access to FAST lanes for truckers on the northern and southern borders.

In addition, we have been informed that inspections as a whole have increased in the last six years (which would explain why C-TPAT members have not observed a noticeable decline in inspection rates), but we have not heard of any significant rises in inspection levels for non-C-TPAT members. In any case, it is hard to say whether security inspections have increased or decreased as a result of C-TPAT membership since many types of examinations exist and numerous factors contribute to the selection process. For instance, there are more contraband-enforcement exams along southern land borders. With this in mind, it is difficult to determine whether shifting inspection rates are related to security issues and C-TPAT membership.

5. In your testimony, you state the benefits being offered to C-TPAT participants continue to be elusive. What steps should CBP take to fix this problem?

Response: CBP should work with the trade community, and specifically its C-TPAT partners, to identify additional benefits for C-TPAT participants. Similar to how CBP worked with C-TPAT participants in updating the minimum security requirements for each enrollment sector, it should do the same to identify new benefits as well. In terms of specific recommendations, JIG strongly endorses the negotiation of mutual recognition agreements for international security programs such as C-TPAT, as well as expanded recognition domestically between various government agencies. Additionally, C-TPAT needs to be seen as a viable, cost-effective program. CBP's own Cost-Benefit Survey showed that less than one-third of the respondents found benefits of C-TPAT to equal or exceed the costs from the program. As security requirements continue to intersect with facilitation issues, CBP must work with its C-TPAT partners to develop tangible commercial benefits to C-TPAT membership.

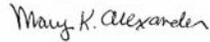
Resumption of Trade

6. *What do you think of the existing plans for trade resumption in the event of an incident?*

Response: The JIG membership holds widespread concern about any existing plans for trade resumption in the event of an incident, and much of this worry stems from the fact that we have been provided only limited information about any such plans. We believe, however, no universal approach is applicable to every situation. As a result, we believe it is important that the Coast Guard and CBP conduct exercises that test different port incident recovery scenarios. We emphasize the need for effective and coordinated communication between government agencies and the private sector in the event of any incident or disruptive event. In any incident, industry needs to know who is in charge, what information is needed from the trade community, and how will it be provided. We understand that CBP and the Coast Guard are working on a joint communications plan to use during an incident, and we commend them for this effort. We would welcome opportunities to provide input, and we look forward to learning more about their plans at the appropriate time.

Mr. Chairman, thank you once again for providing a platform for discussion of the SAFE Port Act and the programs that either have resulted or been affected by this legislation. We would be happy to provide any additional information as you request it, and we look forward to maintaining a dialogue with you and your Committee.

Best Regards,



Mary Alexander, Chair
Joint Industry Group

Attachment 1: JIG Letter to DHS Voicing Concerns about GTX

August 2, 2007

The Honorable Michael Chertoff
 Secretary for Homeland Security
 US Department of Homeland Security
 Washington, DC 20528

Dear Secretary Chertoff:

Over the past several years, the trade community has been pleased to be included as a partner in discussing, developing, and implementing numerous policies designed to improve homeland security. Including the private sector in policy development has produced programs that have been integrated into business practice without overly adverse effect.

Today we note our serious reservations about the possible development of a third-party data warehouse, or what is referred to as the "Global Trade Exchange." The development of this program, which is a highly complicated concept, will undoubtedly raise a number of issues related to commercial competitiveness and global security. For this reason, the international trade community must be consulted in the program's development before it or a pilot is instituted.

The Joint Industry Group (JIG) is a coalition of importers, exporters, shippers, carriers, customhouse brokers, trade associations, service providers and law firms with an active involvement in global commerce. JIG frequently engages Congress and the Administration on a variety of international trade-related issues. We work particularly closely with Congress to promote international trade policy that reflects the needs of both government and the private sector.

Some of our immediate concerns about the adoption of the Global Exchange concept include:

- The vast amount of information stored within an enormous data warehouse, managed by a private entity, will be difficult to protect. Given the sheer volume of the data and complexity of the electronic protocols, there is a significant potential for leaks. The ability of unauthorized parties to surreptitiously obtain information from the system will inevitably result in harm to both homeland security and the competitiveness of US business.
- International trade is a highly complex area. Companies are constantly searching for new business opportunities and markets. Companies are extremely hesitant to share confidential information with outside parties, including foreign governments, because it will almost always be shared with competitors. The inability of companies to protect their own confidential data is a recipe for commercial disaster.
- Sharing confidential business data with foreign governments must be carefully considered, especially since the US will have little or no control over how the information will be used or disseminated. At this time, we are unaware of any means to ensure that information shared by CBP with a foreign government will be protected or secured against distribution to a business competitor. Will extraterritoriality of US law be enforced? Will data be protected through the WTO and would action through the WTO be sufficient? This must be addressed. If any foreign government acts in a manner that undermines the integrity of the Global Trade Exchange, the effects on US industry would be disastrous.
- In addition to the numerous commercial concerns the Global Trade Initiative creates, it also establishes security concerns. By trusting a large amount of data to the care of the private sector and sharing it with foreign governments, a number of uncontrollable elements will be introduced to the system. A breach of any of these levels could carry significant consequences for the security of our border.

- In light of other data-oriented programs already implemented or under development, such as the “10+2” program, we question the necessity of the Global Trade Exchange. While we understand the importance of collecting data elements to develop more accurate risk profiles, at what point do the expanded requirements become unnecessary or duplicative?
- The implementation of the Global Trade Exchange may violate current US laws, such as the Trade Secrets Act (18 USC § 1905).

This proposal has very serious ramifications to the competitiveness of US companies engaged in global trade. Unlike previous rulemaking by DHS, FDA, USDA, USCG, and CBP, there does not appear to be a plan for input from the commercial stakeholders on the data warehouse concept. We strongly urge you to consult with the trade before moving ahead with the proposal. Failure to do so could result in the loss of trade stability and a significant erosion of confidence in CBP and DHS.

Thank you for the opportunity to provide these comments. We remain available to you and your staff for any clarification.

Sincerely yours,

Mary K. Alexander
Mary Alexander
Chair, Joint Industry Group

CC: Michael Jackson, Deputy Secretary of Homeland Security, DHS
Stewart Baker, Assistant Secretary for Policy, DHS
Alfonso Martinez-Fonts, Assistant Secretary for Private Sector, DHS
W. Ralph Basham, Commissioner, US Customs and Border Protection
Bennie G. Thompson, Chairman, House of Representatives Committee on Homeland Security
Joseph Lieberman, Chairman, Senate Committee on Homeland Security & Governmental Affairs
Carlos M. Gutierrez, Secretary, US Department of Commerce
Susan C. Schwab, Ambassador, US Trade Representative

RESPONSES FROM WADE M. BATTLES FOLLOWS:

Questions from the Honorable Bennie G. Thompson, Full Committee Chairman:

Customs and Border Protection Staffing

1. Please tell us more about the significant CBP staffing problems that are occurring at the Port of Houston and the Houston Airport System. Based on your written testimony, it appears that CBP has not properly provided the number of officers needed at the Port of Houston and the Houston Airport System.

Grants

2. In your written testimony, you highlight some significant problems with the existing port security grant program. Please tell us more about the problems you have had in getting approval to commit these funds.

TWIC

3. According to your testimony, TSA underestimated the number of TWIC applicants by 320,000 in the Port of Houston. That is a significant number. Did TSA give you any explanation on how they came up with their original number?
4. In your written statement, you also say that there has been no significant efforts yet by TSA to notify and educate port stakeholders by TWIC. What steps have you taken to overcome TSA's ineptitude?

PORT OF HOUSTON AUTHORITY

EXECUTIVE OFFICES: 111 EAST LOOP NORTH • HOUSTON, TEXAS 77029-4327
MAILING ADDRESS: P.O. BOX 2562 • HOUSTON, TEXAS 77252-2562
TELEPHONE: (713) 670-2400 • FAX: (713) 670-2429



WADE M. BATTLES
Managing Director
(713) 670-2453

December 26, 2007

The Honorable Bennie G. Thompson
Full Chairman
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

Dear Chairman Thompson:

Reference to the questions you forwarded to me from my written testimony on "SAFE Port Act : Status of Implementation One Year Later dated October 30, 2007. Please see my responses stated below as requested.

#1 Customs and Border Protection Staffing: Historically in Houston Custom and Border Protection (CBP) has maximized the use of their officers by shuttling them between assignments at the Seaport and the Airports. But seaport operations are becoming more and more of a 24/7 operation. With congestion challenges and with the desire to reduce truck traffic during rush hours, the Port of Houston has been required to operate our container gates much later into the evening than before. In order for the container gates to be operational the CBP Radiation Portal Monitors (RPM) must be manned and operational. This has put additional personnel and overtime demands on CBP that were exacerbated by the shuttling of officers between the seaport and airport.

After discussions with the local Director of Field Operations about the problem he separated the two operations into two distinct ports of entry with each having its own Port Director and CBP staff officers. This has greatly improved the situation but overtime for the officers in order to sustain the late gate and weekend operations will continue to be a challenge.

#2 Grants: As indicated in my testimony, at the time when a port initially applies to DHS under the Port Security Grant Program for federal funding of a port security project, the port is required to provide detailed scope and budget information. DHS then notifies the port that as to whether its application has been approved. That notification has occurred typically severally months after the application deadline date.

The port then receives from DHS/FEMA a "Cooperative Agreement" with certain "Special Conditions". Two of the Special Conditions are as follows:

The grantee is prohibited from obligating, expending or drawing down funds provided through this award until the required Budget Detail Worksheet and Budget Narrative are reviewed and approved by the Office of Grant Operations (OGO) and a Grant Adjustment Notice (GAN) is issued removing this special condition.

The grantee is prohibited from obligating, expending or drawing down funds provided through this award until all applicable programmatic documents are provided to and approved by the program office and a Grant Adjustment Notice (GAN) is issued removing this special condition.

To clarify all this, here is an example of the process in Round 7 of the Port Security Grant Program that we have experienced:

1. Application submitted by Port of Houston Authority to DHS/FEMA: March 2, 2007;
2. DHS/FEMA press release notifying ports of selection (grant awards): May 8, 2007;
3. Cooperative Agreement received from DHS/FEMA by Port of Houston Authority: August 8, 2007;
4. Return of Cooperative Agreement (indicating the 36-month project time period commenced June 1, 2007) by Port of Houston Authority to DHS/FEMA: August 13, 2007;
5. Port of Houston Authority is yet waiting to receive notice of GAN releasing Special Notifications. We understand that this notice will not be forthcoming until approximately February, 2008, thus resulting in a diminution of the 36-month time period for implementation of the project by approximately nine (9) months (June 1, 2007 to February 28, 2008).

The approvals required under the Special Conditions in the Cooperative Agreement relate to information that the DHS/FEMA has received with the port's initial application. However, DHS/FEMA withholds approval of this information until, as in our example, some 10 months after notification of award has been sent out by DHS/FEMA to the port.

Since the Special Condition requires DHS/FEMA approval of the information prior to a port's "obligating, expending or drawing down funds provided through this award until the required [scope and budget information] are reviewed and reapproved" by DHS/FEMA, a port is effectively prevented from commencing its procurement process to obtain a contractor to implement the security project until it receives the GAN.

In short, this process is preventing ports from commencing the necessary procurement process until an unacceptably lengthy time after award of a security grant project and, accordingly, the project time frame is typically reduced to a little more than two years – often not enough time to complete many of the projects undertaken with in the time frame allocated.

#3 TWIC: The original estimate on the number of TWIC cards needed in Houston was done by Bearing Point about two and a half years ago. All though I am not privy to the specific methodology they used in developing their numbers, in my discussion with some of the 150 private MTSA regulated facilities that align the Houston ship channel, it is evident that Bearing Point vastly underestimated the number of workers within these facilities that would require a TWIC. Because many of these refineries included their whole facility within their "secure area" footprint, every employee working at the facility would require a TWIC card. For example the East Harris County Manufactures Association estimated that they would need 180,000 cards for their employees and contractors. Since testifying, the Coast Guard has redefined "secure" areas and has allowed facilities to reduce the footprint of their secure areas. This will reduce the number of cards required but the number for the Port of Houston will still be over 200,000 cards vs. the original estimate of only 35,000.

#4 TWIC: TSA has relied on the industry to get the word out about TWIC and industry associations, the unions, and public port authorities have initiated an aggressive public information program. Informational flyers have been inserted with pay checks, flyers have been given to drivers as they enter our facility. We then quiz them as they leave the facility: did you read the flyer, do you know what it means, and do you understand that without a TWIC you will not be able to do what you just did – i.e., enter unescorted into a secure area to pick up or deliver cargo. Those transportation workers who daily work on the docks for the most part know of and understand the requirements of TWIC. Our concern is for those individuals who do not on a regular basis come to the port but whose services are necessary and it is impossible or extremely impractical to provide them escorted access. This group includes vendors, equipment technicians, non-local truck drivers, literally thousands of workers. For example the driver delivering

- 4 -

and picking up waste dumpsters will have to have a TWIC, the forklift mechanic and or sales person will be required to have a TWIC, the vending machine vendor, the FTD florist who delivers bon voyage bouquets waterside to the cruise ship will all need a TWIC. It is this whole class of workers that are completely ignorant of the TWIC requirement until they arrive at the port or a MSTA regulated facility. And finally there is a false perception that a TWIC will be required only for those who work on a "port" and specifically only those handling containers. There is very little understanding in the general population about what MTSA regulated facilities are, and how TWIC will impact access to them.

In conclusion, I trust that I have provided sufficient information to clarify my previous testimony and if I can provide any further information or clarification, please do not hesitate to contact me.

Sincerely,



Wade M. Battles

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON
HOMELAND SECURITY

RESPONSES FROM ROBERT F. BLANCHET

Question 1: As with the TWIC program, TSA has underestimated the annual turnover rate of truckers. Please provide us with more information about this turnover and can you explain how TSA came up with such flawed numbers?

Response: The TSA lumps truck drivers in with all port workers. Most port workers are represented by one of several port unions and have good, family sustaining jobs with good benefits and pensions. It is not surprising that these workers have a relatively low turnover rate. Unionized truck drivers have a turnover rate of only 3% per year.

But according to figures compiled by the American Trucking Association, the turnover rate for owner-operators (who are not represented by unions) is 120% per year. The ATA has never provided figures that break out port drivers from other owner-operators, but everyone involved in port (except the ATA which is justifiably feeling defensive that their member companies have such an appalling retention of drivers) estimates that the figure is HIGHER for port drivers than for the over-all class of owner-operators.

It is easy to see how the TSA came up with such flawed numbers. What is inexcusable is that after we informed them of this problem and their bad numbers some 18 months ago, they did nothing to correct the numbers or justify them.

TWIC

Question 2.: According to your written testimony, a TWIC can be forged with in 498 hours. **What steps should TSA be to prevent this from occurring?**

Response: There is no way to keep a TWIC card from being forged to the extent that Commercial Drivers Licenses are being forged, a thriving industry in many port cities. The only way to foil this is to install the electronic readers concurrent to the roll-out of mandatory use of TWIC cards. The problem comes from the system of having guards, clerks and other officials take a quick look at the cards of CDL holders as the truck rolls through the gates of marine terminals. No electronic readers: No port security. It's that simple.

Question 3.: **Please tell us more about the appalling security loophole that TSA has created which allows credentialed drivers to containers out of the port and hand them off to other drivers which are not credentialed.**

Response: Tank haulers and hazardous waste haulers all need endorsements on their licenses (with FBI background checks) regardless of where they are working. For some reason, TSA only requires port workers and truck drivers who haul containers to have TWIC credentials when they are in a port. Yet the problem of containers possibly carrying into a port is discounted to concern only the driver who hauls the container the last few feet through the gate.

We have talked about this with lower level TSA and Coast Guard officials who all see the problem and, if it was up to them, would like to see a requirement that anyone hauling an intermodal container of having access to it either at a seaport of an off-dock facility, including rail yards and container yards and repair facilities, should be required to be TWIC credentialed. We can take you to any port city in the United States and show you hundreds, if not thousands, of containers parked overnight outside the port gates in streets and off-dock yards waiting to be brought into the port or to some inland destination, possibly for transshipment through another port.

Question 4.: **Do think that there are enough enrollment centers and if not, what more should TSA do to minimize the impact on port workers?**

Response: It is too early to tell if there are enough enrollment centers. The TSA has just begun to open centers at the larger ports with deadlines for applying for the TWIC cards still months away. Time will tell.

Question 5.: **How would it be for me to get a fake TWIC card?**

Response: We will check to see if the underground "document industry" has begun providing these yet or if they are waiting until closer to the time when the TWIC card is mandatory.

Question 6.: The State of Florida has a requirement for a State access card. This seems duplicative to me as I thought the TWIC program was to create uniformity throughout the system. **Should the federal TWIC program pre-empt the state program and if so, why?**

Response: The idea of a Florida State access card was to avoid having port truck drivers pay for purchasing ID cards at each of the Florida ports. Under the TWIC system, individual ports as well as states are allowed to have a parallel credential system. We believe this is partly a hidden tax for truck drivers and partly a gift to the low paying motor carriers who employ the drivers who haul containers.

Here is an example: If a port truck driver in Miami, Florida loses his Port of Miami credential he is required to pay \$25 for a replacement. But if he doesn't lose it, and simply changes jobs to go to work for a different motor carrier, he is required to pay \$70 to get a new card.

QUESTIONS FROM THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON
HOMELAND SECURITY

RESPONSES FROM CHRISTOPHER KOCH



December 21, 2007

The Honorable Bennie G. Thompson
Chairman
Homeland Security Committee
U.S. House of Representatives
Washington, D.C. 20515-6480

Dear Chairman Thompson:

Thank you for the opportunity to testify before your committee on the "SAFE Port Act: Status of Implementation One Year Later" on Tuesday, October 30, 2007, and for your letter of December 13th asking the World Shipping Council to respond to several additional, follow-up questions.

The Council is pleased to try to be of assistance to the Committee in these efforts. The following are responses to the Committee's questions.

Cargo Security

Committee Question: Please provide us with information about the concerns you have with the GTX initiative.

Response: Despite various requests from the trade community to the Department of Homeland Security for consultation on the Global Trade Exchange (GTX) initiative prior to commencing any kind of procurement or pilot process (including an October 12, 2007 request for such consultation to the Department from COAC), the Department issued its GTX solicitation without such consultation. Such consultation with industry may have resulted in a clearer understanding of what the Department was trying to do and in a clearer proposal. In any event, it is unfortunate that the Department chose to proceed on this effort without meaningful consultation with the trade.

The GTX "statement of work" that accompanied the solicitation for GTX pilot projects raises a number of questions about the initiative. The following are some of the initial issues or questions that we can identify at this time:

1. The need for a clearer explanation of what additional information the initiative is trying to obtain. The specific data to be collected is imprecise and vague in the statement of work. The statement of work states that prototypes "shall" include "supply chain data from the point of initiation of the commercial transaction through the logistics and financial components of the final consumer destination and acceptance of the cargo

and closure of the financial obligation (heretofore described as "End-to-End Supply Chain Data Coverage")." It also states that prototypes "shall include the collection and fusion of commercial security data including but not limited to RFID status messages, container security device readings, and radiation detection data." It also states "GTX Data shall include all applicable modes of transportation including sea, air, rail and truck for ... relevant supply chains."

This would be an enormous amount of data. We assume that pilots are not expected to include all such data, and that there will be latitude of undefined extent provided regarding what data is included in the pilots.

It is surprising that such an initiative of this nature from the government would not be more specific about what additional data is being sought for the purpose of improving the government's cargo risk assessment capabilities.

2. Is GTX an initiative that is intended to supplement government information systems with information not presently received via regulatory filings, or is it also a system that will serve as way to fulfill regulatory information filing requirements? The foundational concept articulated for the GTX initiative has been that the data to be provided to the government via GTX is data that is not currently available or provided to the government via regulatory filings. This was stated by DHS repeatedly prior to and in the solicitation. For example, the statement of work states: "GTX is envisioned as a privately operated, self-sustaining (e.g. user-fee based) trade information system that will collect commercial transaction data not currently available to [the U.S. Department of Homeland Security.] "

The solicitation also states, however, that the pilots are expected to: "Ensure collection and transmission of CBP's proposed Security Filing data to CBP automated programs." (page 11) This Security Filing data obviously will be available to the government as soon as the Department completes its "10 plus 2" rulemaking. This would indicate that the GTX system would actually be more than a system to provide governments with shipment data that they do not currently possess. It would be a system that would also need to be designed to file data for shippers for regulatory compliance with "10 plus 2" data filing obligations.

Conceptually, the GTX statement of work seems to anticipate that it is a short step from that to a system that could file information into other governments' customs systems (which is clearly anticipated in the GTX statement of work). It is unclear whether the Department anticipates the GTX information brokers could then take the next logical step to a system that would also file an importer's merchandise entry information to U.S. Customs (i.e., create a "one step" process for a shipper to fulfill its import and export information filing obligations with the U.S. and other governments by providing all its data to one GTX data broker who would then file it with multiple governments). While this solicitation and statement of work do not clearly elaborate the vision for the GTX system or fully address this set of issues, and while merchandise entry filing is "customs business" that must be done by a customs broker, this issue is likely to be a matter of much interest to the trade as this initiative progresses. This is the kind of issue that would have benefited from consultation with the trade.

3. Coordination with Foreign Governments: Respondents to the GTX solicitation need to identify three foreign government participants (one from the EU, one from the Pacific Rim and one from the Middle East) (page 5). This appears to be a requirement for a contractor to be responsive to this solicitation.

Developing a system that will satisfy not only the U.S. Department of Homeland Security's desire for the provision of unspecified additional trade and shipment information, but other governments' information needs, requires close consultation and cooperation with those governments. It is not apparent that this has occurred. If it has not, such an initiative is likely to raise questions within the governments of the United States' trading partners about the U.S. government's intent and objectives.

The statement of work appears to delegate the responsibility for obtaining foreign governments' consent and participation to prospective DHS contractors. We will not speculate about foreign governments' reaction to the GTX solicitation's approach of "partnering with the trade community and foreign host governments" via a small group of DHS-designated, private, for profit data management companies, but we suspect that foreign governments would have questions about the U.S. government's intentions, and that they would expect to address such significant issues on a government-to-government basis.

4. Confidentiality and Access to Data: The statement of work provides: "During operation of GTX, various governmental, domestic, international trading partners as well as commercial entities will have access to the data, real-time." This raises, but fails to begin to address, a host of significant, legitimate questions about who would have access to what data in a GTX system and under what terms.

It also fails to address whether any sort of commonality is expected amongst potential GTX vendors regarding issues such as data elements and data formatting.

Much of the data envisioned to be included in this system would be commercially sensitive (e.g., supplier information, purchase orders, product cost, shipping costs, payment terms). Failure of the government to even begin trying to define governing principles to address these issues of confidentiality and data access will be a matter of significant concern to parties who might be affected by GTX.

The statement of work is devoid of any guidance on this set of issues and simply states that any vendor responding to the solicitation "shall develop a business plan/model that includes a clearly defined strategy to ensure all data security and privacy concerns are adequately addressed." The statement of work does not even try to identify the "security and privacy concerns." Nor does it indicate whether the concerns are to be met in a consistent way by the various prospective GTX vendors. Responses to the solicitation are due January 22, 2008. Delegating this set of issues to prospective contractors without guidance seems to be a peculiar way to address this matter.

5. Cost and Benefit: The statement of work states that the GTX system has to be financially self-supporting (i.e., no cost to the government), meaning that such systems presumably would be viable only if fees are charged to those providing the information to GTX. Thus, there is presumably a cost to participate.

If participants are to incur those costs, it would be helpful to identify the resulting benefits of participation. The Department has not identified any benefits to shipper/supplier/carrier participation in a GTX pilot or a GTX program.

In addition, it would be helpful if the Department were to provide some assessment of the benefits to its security programs and capabilities that would result from these proposed pilots.

Finally, while we understand that the GTX pilots are voluntary, DHS has not been clear about its intent with respect to whether an operational GTX program would be voluntary. We would expect members of the trade community to have questions about a program that would make provision of such data to a for-profit, fee-charging company necessary as a matter of law or commercial practice.

6. Procurement Limitations: DHS's solicitation for the GTX Pilot is being made pursuant to the Department's Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) solicitation process. This process has resulted in no meaningful consultation with the trade, and the statement of work accordingly suffers from a failure to answer questions that will be of obvious relevance to the trade and to prospective GTX vendors.

This EAGLE solicitation process also significantly restricts eligible participants to a small pre-selected group of companies. The rationale for this restriction has not been publicly explained to the Council's knowledge. Interested parties not on the eligible list may have concerns with this.

Some may also find it noteworthy that a solicitation for the development of a pilot system that is intended to involve transmission of the applicable data to other national governments' customs authorities, as well as the U.S. government, would be restricted to a list of U.S. government pre-selected vendors. We would expect that other governments may have questions about this.

7. Vision of GTX System: The DHS GTX pilot solicitation is open to eligible EAGLE solicitation process companies, thus the likelihood of multiple vendor responses to the pilot solicitation is expected.

The DHS solicitation and statement of work are silent, however, about whether DHS envisions GTX to be a program (if it evolves beyond the pilot phase) to be comprised of multiple vendors competing for business, thereby requiring consistency across the various information brokers on everything from the data to be collected to the formatting of the data, or, in the alternative, whether DHS envisions one vendor being ultimately selected to be the GTX information broker. We understand that at least some of the vendors intending to participate in the pilot phase envision the GTX system, if made operational, to be operated by a single designated company, and that participation in the GTX system would need to be widespread if not mandatory by the trade.

This is obviously a highly significant issue that is unaddressed.

8. Role of Ocean Carriers in GTX: We appreciate the Committee's interest in what concerns ocean carriers may have with respect to the GTX initiative. As there was no consultation with the liner shipping industry prior to the issuance of the solicitation, we have only the statement of work to guide our understanding of the Department's intent and objectives regarding information from ocean carriers that would be relevant to GTX. We find the project ambiguous at best and potentially troubling for ocean carriers.

The GTX statement of work states:

- a. "The participants shall include shippers and carriers."
- b. "GTX Data shall include all applicable modes of transportation including sea, air, rail, and truck for the regions identified above for relevant supply chains."
- c. "During the option period, the Contractor shall operate and maintain a GTX system that will:
 - Collect, interrate, transform, display and transmit data from:
 - o Regulated or Unregulated commercial supply chain data (e.g., purchase orders, fulfillment schedules and invoices), and may include Radio Frequency Identification (RFID) status messages from Container Security Devices (CSDs);
 - o Vessel transponder data; and,
 - o Other information regarding production management records, inventory records and advance ship notices from foreign suppliers that the GTX Pilot Contractor may identify as useful."
 - "Have 10 trade participants (shippers and carriers) providing supply chain data regularly (i.e., hourly, daily)."

It remains very unclear, however, what data ocean carriers would have or would be expected to provide into a GTX pilot. Carriers already provide the government with advance Notices of Arrival, vessel manifests, "24 Hour Rule" advance shipment submissions, and have AIS vessel transponders that communicate with Coast Guard receivers. Furthermore, in the very foreseeable future, ocean carriers will be transmitting long range vessel tracking information to the government via the Long Range Identification and Tracking (LRIT) vessel tracking system, and will be submitting their electronic container status messages (CSMs) and vessel stowage plans pursuant to the "10 plus 2" regulations.

"Vessel transponder data" is a poorly conceived element for inclusion in GTX, because AIS transponders already provide the U.S. Coast Guard with vessel transponder data close to the U.S. coast, and the LRIT system under development by the International Maritime Organization and by various nations (and strongly supported by the U.S. Coast Guard) pursuant to a specific international agreement will provide greatly expanded vessel identification information for all arriving vessels when it becomes operational December 31, 2008. We have no idea why GTX would or should be considered a duplicative system for receiving "vessel transponder" data. The GTX statement of work should not be interpreted as requiring vessel transponder data to be a GTX data element, when the Department is already collecting it under an existing Coast Guard system and is working with the industry on the implementation of the next generation system.

In addition, we can identify no reason why an ocean carrier would want to provide CSM and stow plan data (under the imminent "10 plus 2" regulations) via GTX (especially when a fee of some kind would probably be involved via GTX) rather than transmit such data directly to CBP in compliance with the regulations.

Upon our inquiry with CBP, the agency has emphasized that any ocean carrier participation in these GTX pilots is purely voluntary. We also understand that, notwithstanding the language of the GTX statement of work, ocean carrier information and/or participation is not necessary for a party submitting a response to this solicitation to have a qualifying submission. This would be a helpful clarification, which we have requested from CBP.

In summary, whatever GTX might become as a system to obtain additional shipper and shipment information, we can at this time identify no reason why GTX would be an attractive way for ocean carriers to provide any data they control to the government. If the U.S. government wants additional information from ocean carriers, we believe the government should inform the industry of what that additional data would be and then discuss with the industry how it may transmit that information directly to the government, rather than sending it through a select group of for-profit companies.

9. Container Security Devices: The GTX statement of work provides that the system "may" include Radio Frequency Identification (RFID) status messages from Container Security Devices (CSDs). While recognizing that is an optional portion of the concept, we note that DHS has recently issued CSD specifications for several pilot project solicitations.

We note that those specifications provide that the CSD specs for these pilots only will detect whether the right container door has been opened, not the left door.

More importantly, the specifications provide that the CSDs used in these pilots may generate a permissible false alarm rate of 4%.

This is far above what senior Customs and Border Protection officials have earlier publicly stated would be an acceptable error rate. And it is twenty (20) times greater than the acceptable error rate recommended in the draft CSD specifications produced by the Department's Science and Technology Directorate.

Technology vendors, marine terminal operators and carriers all agreed during the development of the ISO standard for electronic seals that a 99.99% accuracy rate was an appropriate specification, and this is the ISO specification for e-seals.

We do not understand how the Department could determine that a 4% error rate could be considered a defensible specification for CSDs.

We wish to convey to the Committee our strong view that, whatever else occurs during the planned pilot tests of CSDs, testing devices with a permissible 4% false alarm rate is not testing a technology that can have practical application in the commercial operating environment. Such device specifications would be wholly unacceptable for widespread commercial application.

Summary: GTX appears intended to be a "big idea" concept that seeks to transform how international trade is documented and how information is shared amongst trading partners and governments. An idea that "big" requires deliberation, care, clarity, and consultation in order to identify the objectives, the significant issues that must be addressed, and the process for addressing those issues.

Since September 11, U.S. Customs and Border Protection has a history of effective consultation and communication with the trade on emerging security initiatives, such as the development of the C-TPAT program and the "10 plus 2" regulations. The present GTX solicitation and statement of work were undertaken without consultation with the trade and raise more questions than they answer.

Customs-Trade Partnership Against Terrorism

Committee Question: According to Ms. Alexander, C-TPAT benefits have been elusive. Do you support Ms. Alexander's statement? What benefits have your Members received?

Response: We understand that C-TPAT importers receive the benefit of reduced Customs inspections of their shipments. CBP statistics on these inspection rates should help the Committee determine the magnitude of that benefit, but our understanding is that the difference is significant and meaningful.

Ocean carriers receive no benefit from CBP for C-TPAT participation. C-TPAT participation by ocean carriers is based on commercial motivation to do business with C-TPAT importers.

Resumption of Trade

Committee Question: What do you think of the existing plans for trade resumption in the event of an incident? Are you confident that the U.S. government will be able to respond in a timely manner such that the impact on your members, the international liner shipping industry, is minimal?

Response: We are not aware of the government's existing plans for trade resumption in the event of an incident.

The government's response to a security incident is likely to be highly dependent on a host of variables, including the facts of the specific incident, and the reaction of Members of Congress and other public leaders. Further, we have little predictive insight into the reaction of state and local governments or the federal government's plans for how to deal with state and local governments when trying to implement trade resumption policies. Accordingly, the industry has little ability to predict or to be confident of the government's response.

We understand that Customs and Border Protection and the Coast Guard are finalizing an agreed process for how they would communicate and coordinate during an incident response. This is a positive step. We further understand that this communication plan envisions establishing a communication mechanism between the agencies and the various maritime industry sectors, and that the World Shipping Council is envisioned to be a conduit for communication with the international liner shipping industry. The Council is very willing to try to be of assistance to the government in this regard.

Transportation Worker Identification Credential

Committee Question: As you have heard today, criminal elements are already trying to figure out ways to create fraudulent TWICs. In your opinion, how will the implementation of the TWIC reader improve the security of the TWIC program?

Response: We do not know how difficult it would be to create a fraudulent card that would resemble a TWIC. While it is conceivable that someone may be able to create a false TWIC card to be used as a "flash pass" in the initial stages of the TWIC program, creating a TWIC card that would also defeat a biometric TWIC reader would be very difficult. Transportation Security Administration representatives have informed the National Maritime Security Advisory Committee that it is not something that could happen under the specifications being used for the card and readers. On an issue such as this, which requires substantial technical card creating and card reading knowledge, we defer to the professional judgment of TSA.

###

The Council again wishes to thank you for the opportunity to present these views to your Committee, and we remain ready to work with the Committee in a common effort to advance sound maritime security enhancements.

Sincerely yours,



Christopher Koch
President

○