H.R. 4954, THE SAFE PORT ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 16, 2006

Serial No. 109–69

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

36–696 PDF WASHINGTON : 2007

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

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
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
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
PETER T. KING, New York *(Ex Officio)*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity:
Oral Statement 1
Prepared Opening Statement 2
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity 3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security 5
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 41
The Honorable Jane Harman, a Representative in Congress From the State of Caifornia 6
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 32

WITNESSES

Mr. Jayson Ahern, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security:
Oral Statement 7
Prepared Statement 9
Captain Brian Salerno, Deputy Director, Inspections and Compliance, United States Coast Guard, Department of Homeland Security 15
Mr. Eugene Pentimonti, Senior Vice President, Government Relations, MAERSK Inc:
Oral Statement 16
Prepared Statement 19
Mr. Noel Cunningham, Principal, MARSEC Group:
Oral Statement 21
Prepared Statement 23

H.R. 4954, THE SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT

Thursday, March 16, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 12:18 p.m., in Room 311, Cannon House Office Building, Hon. Daniel Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Sanchez, Dicks, Lofgren, Jackson-Lee, Thompson, and Harman.

Mr. LUNGREN. [Presiding.] The committee will come to order.

We meet today to hear testimony on H.R. 4954, the Security and Accountability For Every Port Act, that is the SAFE Port Act of 2006.

We will gather testimony from port security experts and industry stakeholders on what Congresswoman Harman and I, as well as others on this committee and subcommittee, believe to be a very important piece of legislation.

This Tuesday, Ms. Harman and I, joined by 48 other members, including Ranking Member Sanchez, introduced the SAFE Port Act. As you can guess by this hearing, we are not wasting any time in making this legislation law. We have been working on this issue of port security for quite some time and are encouraged by the increased urgency with which the issue is now being discussed and considered.

I would like to welcome and thank our witnesses, Mr. Jayson Ahern, the assistant commissioner for the office of field operations in the U.S. Customs and Border Protection; Captain Brian Salerno, the deputy director of inspections and compliance, the United States Coast Guard; Mr. Eugene Pentimonti, the senior vice president for government relations for Maersk, Inc.; and Mr. Noel Cunningham, the principal for the MARSEC Group and former director of operations and emergency management for the Port of Los Angeles.

The Security and Accountability For Every Port, or SAFE Port Act, is a comprehensive proposal to strengthen the maritime transportation system through a layered security strategy that builds on already-existing initiatives to secure the supply chain from the point of origin to delivery in the United States. I believe the administration has established a foundation upon which we are building, but the building upon that foundation is urgent.

This legislation focuses on improving security both at home and abroad by expanding capabilities, maximizing available resources, and pushing our borders outward.

The legislation has three key ideas: first, enhancing security at U.S. ports by establishing a $400 million port security grant program with dedicated funding from custom duties; requiring terrorist watch list checks of all port employees with secure access at ports; and establishing additional joint operations centers and furthering the deployment of radiation detection equipment.

Second, preventing threats from reaching the United States by authorizing and improving two Customs and Border Protection cornerstone security programs: the container security initiative and the customs trade partnership against terrorism.

Third, tracking and protecting containers en route to the U.S. by improving our ability to detect high-risk containers through strengthening the automated targeting system; establishing container security standards; and supporting additional cargo security research and development, including reviving Operation Safe Commerce.

Since September 11, the federal government has invested over $7 billion in port security. There is no doubt that the funding and programs it supported has made us safer and our ports stronger. However, I think no one is satisfied with the past actions and believe that we must do nothing else. In fact, we must move forward with renewed focus and energy to improve our ports.

I look forward to questioning the witnesses about the programs and funding in place currently are working; what impact the legislation will have when implemented, as well as any recommended changes. The committee is putting this legislation on the fast track. Tomorrow, members of the subcommittee will be going to the ports of Long Beach and Los Angeles to review port security operations, and after the March recess, we intend in this subcommittee to mark up this bill.

We have every reason to believe that the full committee will act with dispatch as well. So we would like your help to develop the best legislative proposal possible. Again, I would like to thank the witnesses for being here today and for the work that all of you have done in your respective agencies and companies to protect our ports.

Now, it is my pleasure to recognize the ranking minority member of the subcommittee, the gentlelady from California, Ms. Sanchez, for any comments she may make.

PREPARED OPENING STATEMENT OF THE HONORABLE DANIEL E. LUNGREN

Today the Subcommittee also meets to hold a legislative hearing on H.R. 4954, the *Security and Accountability For Every Port, or "SAFE Port" Act.* We will gather testimony from port security experts and industry stakeholders on what myself and Congresswoman Harman believe to be a very important piece of legislation. This Tuesday, Ms. Harman and myself, joined by 48 other Members, including Ranking Member Sanchez, introduced the SAFE Port Act. As you can guess by this hearing, we are not wasting any time in making this legislation law. Ms. Harman and I have been working on the issue of port security for quite some time now, and are encouraged by the increased urgency with which the issue is now being addressed.

I would like to welcome and thank our witnesses:

- **Mr. Jayson Ahern,** *(pronounced A-hern)* the Assistant Commissioner for the Office of Field Operations in U.S. Customs and Border Protection

• **Captain Brian Salerno,** the Deputy Director for Inspections & Compliance in the United States Coast Guard
• **Mr. Eugene Pentimonti,** *(pronounced pent-i-mont-e)* the Senior Vice President for Government Relations for Maersk (pronounced Mersk) Inc
• **Mr. Noel Cunningham,** the Principal for the MARSEC Group, and formally the Director of Operations and Emergency Management for the Port of Los Angeles

The Security and Accountability for Every Port or "SAFE Port" Act is a comprehensive proposal to strengthen the maritime transportation system through a layered security strategy that builds on existing initiatives to secure the supply chain from the point of origin to delivery in the United States. This legislation focuses on improving security, both at home and abroad, by expanding capabilities, maximizing available resources, and pushing our borders outward.

The legislation has three key ideas:

1. *Enhancing Security at U.S. Ports* by establishing a $400 million Port Security Grant Program with dedicated funding from Customs Duties, requiring terrorist watchlist checks of all port employees with secure access at ports, establishing additional joint operations centers, and furthering the deployment of radiation detection equipment.

2. *Preventing Threats from Reaching the U.S.* by authorizing and improving two Customs and Border Protection cornerstone security programs—the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT).

3. *Tracking and Protecting Containers En Route to the U.S.* by improving our ability to detect high-risk containers through strengthening the Automated Targeting System, establishing container security standards, and supporting additional cargo security research and development, including reviving Operation Safe Commerce.

Since September 11, 2001, the Federal Government has invested over $7 billion in port security. There is no doubt that the funding and the programs it supported made America safer and her ports stronger. However, we can't be satisfied with past efforts and must move forward with renewed focus and energy to improve our ports.

I look forward to questioning the witnesses about how the programs and funding in place currently are working, what impact the legislation will have when implemented, as well as any recommended changes. The Committee is putting this legislation on the fast track. Tomorrow Members of the Subcommittee will be going to the Ports of Long Beach and Los Angeles to review port security operations and after the March recess we intend to mark up this bill. We want your help to develop the best legislative proposal.

Again, I'd like to thank the witnesses for being here today and for the work that you have each done in your respective agencies and companies to protect our ports.

I will now recognize the Ranking Member, Ms. Sanchez, for any opening statement that she may wish to make at this time.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I want to thank our witnesses for coming today to testify before us.

I am pleased that we are finally looking and considering today the important issue of port security. Port security affects us every day. I tell my colleagues all day long that if it comes through the port, it is probably put on a train or it is put on a truck and it goes through all of our neighborhoods. So understanding what is in those containers and what could affect our people is a very, very important issue. The safety, checking these and having a secure trail of where they have been is very, very important to us.

It is also very important from an economic standpoint. I remember a couple of years ago during Christmas when we had the shutdown at the L.A.–Long Beach ports. It cost us almost $2 billion a day, and it wasn't just the California area. A factory in Alabama that does just-in-time and is waiting for parts to construct automobiles will have to layoff its people for the week if the pieces don't come. So it is very, very important from an economic standpoint.

And despite that, I don't think we have done very much from the federal level to help secure the United States ports. I know that

many of our local ports, because they are locally owned either by the city of Long Beach or the city of New York or what have you, have been not only putting up the first plans and methods of trying to secure the ports, but also their own money. So I think it is very important that we have this discussion.

Many of us have been working on this issue for many years. I personally have introduced three separate bills on the issue of port security over the last 2 years, and this committee actually passed what was really the blueprint for this bill that we are going to be discussing today. Unfortunately, it didn't get taken up by the Senate, but now it has. It is coming back, and so now we are going to, I hope, Mr. Chairman, pass a good bill.

I look forward to hearing from our witnesses. I am particularly very interested in your thoughts on the customs trade partnership against terrorism, or C–TPAT. I think that it is a very valuable program, but I am concerned that the Customs Border Protection is granting substantial benefits such as decreases in the targeted risk, to the 63 percent of the C–TPAT members that haven't been validated yet. I am concerned that this administration has been unwilling to request the resources for CBP to complete the validations quickly and thoroughly.

Moreover, as time passes and supply chain technology develops, it may be more difficult for CBP to conduct follow-up validations that may be necessary to ensure that C–TPAT members continue to employ top-of-the-line security procedures.

While you are here today, I would also like to hear what you are doing to get the transportation worker identification card implemented. It is an extremely valuable tool that will increase security at facilities nationwide. Last week, I added an amendment to the chairman's TSA reorganization bill to set hard deadlines of June 1 of this year and June 1 of 2007 for the release of the regulations and the implementation of this identification card.

I am also very interested about an issue that many haven't thought about, and this is the whole issue of independent truckers or the truckers that actually come into the port system. I certainly have seen some of these truckers waiting 4, 5, or 6 hours to get into the ports. I also understand that many of them, we don't have background checks for many of them. So this could be one of the weak links happening at our ports.

Some of them have had to declare bankruptcy because it is very difficult to make ends meet when you are trucking and the rates are low and you are waiting in line and you are not getting through and you are not hauling. You are not making money if you are not hauling. Many of them, I have a feeling, at least in the California area, may be undocumented.

So we have to really consider that these people are getting into our port system. Now, one of the issues that this bill might do is to say that there are secure areas and people without the proper background checks would not be allowed in those areas. But I think any area of our port system is subject to problems with respect to somebody who might want to slow down from an economic standpoint or create havoc from a terrorist standpoint. So I would really like to talk about the trucks or at least bring that up as an issue, Mr. Chairman.

I am pleased to be a cosponsor of the SAFE Port Act we will be discussing today, and which our committee, as you said, Mr. Chairman, will be marking up. I look forward to talking about the specific provisions of that bill and about the issues I just mentioned here.

I thank you for your participation in this important hearing, and I yield back.

Mr. LUNGREN. I thank the gentlelady for her comments.

It was my intent at this point in time to yield to the chairman of the full committee for a statement, but the last time I saw the chairman he was wearing a green tie and surrounded by people named O'Hearn, Murphy, O'Connell. But I think he is going to try and get here after he settles with those folks.

So the chair will now recognize the ranking minority member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he may have.

Mr. THOMPSON. Thank you, Mr. Chairman. I hope our chairman didn't have something in the cup that was green, too.

[Laughter.]

So he may or may not be here, but I am sure he will be here.

Thank you again for the opportunity to give my comments. I would like to applaud Congresswoman Harman and Chairman Lungren for this important piece of legislation. I would also like to give the ranking member of the subcommittee, Congresswoman Sanchez, who has sort of been out front on the port issues for quite a while, her support for this effort also.

It is unfortunate that this issue was crystallized with the Dubai port incident. I think we all want to make our ports safe, but we have to do it systematically and not knee-jerk. So this act is the beginning of trying to make some of that happen.

I would like to say, too, Mr. Chairman, that we have enough history from both the IG and GAO who talk about the critical port security gaps that we have here in this country. So this legislation and other legislation is going to be absolutely necessary if we are to make our ports safe. The public will demand it. I think they will say procrastination has gone on long enough. If we have the best minds available identifying what we need to do, we need to get on with it. At some point, we have to do that.

I look forward to the testimony, not only from the Coast Guard and CPB, what they have to add to this piece of legislation, but Mr. Chairman, I want to make the ports safe. We have men and women who work every day on them. We have a lot of cargo that comes in, and we absolutely cannot accept second best. We have to have the best system available, and I look forward to the testimony.

Thank you.

Mr. LUNGREN. I thank the gentleman for his statement.

Without objection, the chair recognizes Ms. Harman—although not a member of the subcommittee, a member of the full committee—for any comments she may make and for participation in the hearing today.

Ms. HARMAN. Thank you, Mr. Chairman, and thank you, Ranking Member Sanchez and Ranking Member Thompson, for your generous remarks.

I am very happy to sit in on this subcommittee hearing to speak for a bill that I believe will become law. It is hard to say something like that in this Congress, but I actually think we have a live one here. The notion that this bill was introduced on Tuesday, the day of the birth of my first granddaughter, and will be the subject of hearings today, and is tentatively going to be marked up at the end of this month, is I would say a legislative miracle.

The other piece of the good news story is that a very similar bill has been introduced on a bipartisan basis on the Senate side by Senators Patty Murray, Susan Collins, Joe Lieberman and Norm Coleman. And that bill will be the subject of hearings in April, and also is expected to move. So it is a silver lining from Dubai ports issue that Congress has now focused on this, but many of us, as Ms. Sanchez said, have been focused on this for a very, very long time.

As this bill moves, I hope that the best ideas that the House has had in a variety of bills will be incorporated and we will do our best job to come up with a strategy and adequate funding for true port security.

I want to welcome particularly, if I might, one of the witnesses, one of my all-time favorites. He has a different hair style now, but Noel Cunningham did an extraordinary job in his role as director of operations and emergency management of the Port of Los Angeles.

He and others, I would salute particularly two groups that I think have had the major role for making the ports of L.A. and Long Beach much safer than they were before 9/11. One of those groups is not here. The Coast Guard has played a magnificent role in pulling all of us in government together, but the other group that I would like to salute, and they are here in force, is the ILWU, a union of patriots who operate the cranes and do other things that are essential at our ports.

Some astute, or maybe it was the same one, but astute crane operators noticed at the Port of L.A. fairly recently human beings getting out of a container that had just been downloaded from a ship. The bills of lading said "clothing," but obviously the contents were, in this case, immigrant stowaways coming here to seek a better life. Those contents could have been terrorists or could have been the components for a radiological bomb, and that is what this committee worries about, all of us do.

And that is why a strategy, which this bill proposes, to authorize the two big programs that check whether bad stuff is being onloaded at foreign ports and to fully fund other operations that will make certain that we push our borders out and we know absolutely what is arriving at our ports, is essential.

I would just like to say one more thing. I have personally talked to Michael Chertoff, the secretary of homeland security, about this bill. I have urged him to support the concepts in this bill. I think it would be very helpful if we had DHS on board at the earliest time, and if DHS was part of shaping this into the best possible legislation. After all, Secretary Chertoff is a systems thinker. He knows that port security is the Achilles heel of our transportation security approach because it is so underfunded.

And I really think, Mr. Chairman, with the help of all the members of the committee, especially Ms. Sanchez, that we can shape this into something that will be the right answer for the right problem at the right time.

I am very pleased to be part of this hearing. Thank you very much.

Mr. LUNGREN. Thank you, Ms. Harman.

Obviously, under the rules, any member of the committee may submit an opening statement for the record. We are pleased to have this distinguished group of witnesses before us today on this important topic. Let me just remind you that your entire written statements will appear in the record.

The chair recognizes Mr. Jay Ahern for 5 minutes to testify as our leadoff witness.

STATEMENT OF JAYSON AHERN, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. AHERN. Thank you very much, Chairman Lungren and other members of the committee here today.

My name is Jay Ahern. I am the assistant commissioner for field operations within Customs and Border Protection. I am also very pleased to be here with my colleague Captain Salerno from the Coast Guard, as well as our partners from the private sector here today, to talk about the security of our country and specifically maritime cargo security.

Mr. Chairman, I specifically want to also commend you and your hard-working staff for bringing visibility to the cargo and port security issue long before the recent attention given to this issue through the Dubai Port World issue, and other members of the panel as well. I also am very appreciative of the strong support of CBP's efforts to secure the global supply chain in America's ports.

Certainly, it is known that Customs and Border Protection's priority mission is homeland security. As America's frontline border agency, CBP is charged with the extraordinarily important mission of keeping terrorists and terrorist weapons out of our country. Securing America's seaports and the global security of the cargo system continues to be a work in progress.

I can say to you that our nation's 322 ports of entry in the global supply chain are far safer today than they were before the terrorist attacks of September 11. Since 9/11, our nation has made great strides toward securing America's borders, protecting trade and travel, and ensuring the vitality of our economy.

Customs and Border Protection, along with other government agencies, along with our private sector and international partners, have instituted unprecedented programs to secure our seaports and the cargo moving into those seaports. We are pleased to see that many elements of our cargo security strategy are contained in the SAFE Port Act.

It is also important to note that as I talk about our five interrelated elements of our strategy that none of our programs existed before 9/11. And also before 9/11, four separate agencies in three different departments of government were responsible for protecting our borders. Today, the personnel and the functions from all

border agencies have been unified into one border agency within one department and government.

The very existence of Customs and Border Protection makes us vastly better able to protect our nation from external threats. Shortly after 9/11, the United States Customs, now Customs and Border Protection, developed a layered defense strategy to secure the movement of cargo, without stifling legitimate trade and travel so important to the economy of this country. That strategy is built on five interrelated initiatives that extend our zone of security beyond our physical borders. We did not want our ports of entry to be the first time we had an opportunity to engage with a sea container coming into this country.

The first is advance information of who and what is headed to the United States from abroad. That is the 24-hour Trade Act rules that require advance electronic information on all cargo, 100 percent of that cargo being shipped to the United States. The second element is taking that information and putting it through the automated targeting system housed at the National Targeting Center just outside of Washington, D.C.

We use that information and we put it through targeting rules based on strategic intelligence to assess risk for terrorism on every cargo shipment headed to the United States. The National Targeting Center is staffed with representatives from Customs and Border Protection, Immigration and Customs Enforcement, the FBI, the Coast Guard, as well as many other federal agencies.

We continue to work to improve our targeting capabilities by enhancing integration of intelligence into our targeting efforts and continue to evaluate the data elements we are currently looking for targeting purposes, and I am glad to see that this act also addresses additional targeting elements.

Third is the use of cutting-edge technology. When cargo arrives at our seaports, CBP uses large-scale X-ray systems, as well as radiation detection devices to screen the containers. At our nation's seaports today, we have 190 radiation portal monitors and 59 large-scale X-ray systems. Before 9/11, there were no radiation portal monitors at our seaports and only 60 large-scale X-ray systems at all of our seaports throughout the country.

A fourth initiative involves partnering with other countries through the container security initiative, or CSI, to screen high-risk containers before they are loaded onboard vessels for the United States. We are currently now operational in 43 of the largest ports in the world.

On March 8, we opened the most recent one in Port Salalah, Oman. These ports handle 74 percent of the cargo containers coming into the United States. Before 9/11, Customs and Border Protection did not have any officers stationed at foreign ports. By the end of 2006, we expect to have officers stationed at an additional seven ports, which would then account for 80 percent of the cargo coming into the United States.

Finally, our fifth initiative involves partnering with the private sector through the customs trade partnership against terrorism, known as C–TPAT. Today's C–TPAT has nearly 5,800 certified members from the private sector, including most of the largest U.S. importers who are working to increase supply chain security from

foreign loading docks to the U.S. port of arrival. More than 10,000 companies have applied to become C–TPAT members and through C–TPAT, CPB reviews the security practices of companies shipping goods to the United States, as well as companies providing services to those shippers.

All these elements we need to continue to improve, and we are continuing to focus on that on a daily basis. But when you take these elements together, these five initiatives and put them in an interrelated strategy and extend our zone of security beyond our nation's borders, we believe we are providing the country greater protection than we did certainly prior to 9/11. As I mentioned before, none of these elements existed before 9/11.

In conclusion, we certainly know that America's borders and the security of those borders is an ongoing and long-term effort. I am very proud of the men and women who work for Customs and Border Protection and within the Department of Homeland Security to secure those ports every day. I am proud of what we have done as a nation and have accomplished in a relatively short time to make America safer, and particularly our seaports more secure, but certainly more needs to be done.

I will be happy to take any questions when it is my time. Thank you.

[The statement of Mr. Ahern follows:]

COMBINED PREPARED STATEMENTS OF JAYSON P. AHERN AND

CAPTAIN BRIAN SALERNO

I. *Introduction and Overview*

Chairman Lungren, Ranking Member Sanchez, Members of the Subcommittee, it is a privilege for the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to appear before you today to discuss the Department of Homeland Security's programs that are fundamental to securing our nation's ports, and maintaining the economic viability of the Marine Transportation System.

CBP, as the guardian of the Nation's borders, safeguards the homeland—foremost, by protecting the American public against terrorists and the instruments of terror; while at the same time, enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws. In FY 2005, CBP processed almost 29 million trade entries, collected $31.4 billion in revenue, seized 2 million pounds of narcotics, processed 431 million pedestrians and passengers, 121 million privately owned vehicles, and processed and cleared 25.3 million sea, rail and truck containers. We cannot protect against the entry of terrorists and the instruments of terror without performing all missions.

The Coast Guard is the Federal agency in charge of maritime security in our ports and waterways. The Coast Guard works very closely with other agencies to pursue a collective strategy of "layered security." Protective measures are implemented overseas within the global trade environment, others are implemented closer to our shores and then still other actions are taken within the U.S. ports themselves. In the overseas arena, the Coast Guard and CBP work together to identify security gaps in foreign ports through our International Port Security Program, which helps CBP position its resources appropriately to most effectively verify high risk cargo prior to loading onboard a ship bound for the U.S. Additionally, the Coast Guard has actively supported CBP on international delegations to develop international standards for supply chain security. The Coast Guard and CBP have also established mechanisms for CBP to obtain the cargo and crew information from the Coast Guard's electronic Advance Notice of Arrival system. This allows both agencies to

conduct vessel screening and targeting operations for high risk vessels bound for the U.S. thereby increasing the layers of protection associated with these vessels before they reach our shores. The Coast Guard and CBP have exchanged liaison officers at CBP's National Targeting Center and at the Coast Guard's Intelligence Coordination Center to facilitate information sharing and operational response coordination when high risk cargo, vessels or crew are identified.

There are numerous other coordination initiatives underway that support cargo security.

The Coast Guard and CBP are working together both on program management and to plan for operational issues associated with "Operation Safe Commerce" project, the DHS container seal regulation project, and both national and local level operational coordination issues to target vessels and respond to threats, among others.

The concept of "layers of security" is complex, involving multiple types of activities to create a network of interdependent, overlapping and purposely redundant checkpoints designed to reduce vulnerabilities, as well as detect, deter and defeat threats. It entails developing security measures that cover the various components of the maritime transportation system, including people, infrastructure, conveyances and information systems. These security measures span distances geographically—from foreign ports of embarkation, through transit zones, to U.S. ports of entry and beyond—and involve the different modes of transportation that feed the global supply chain; and are implemented by various commercial, regulatory, law enforcement, intelligence, diplomatic and military entities. A significant challenge to constructing integrated layers of security is the fact that many of the layers are the responsibility of different agencies. Integrating these disparate maritime security layers involves not only unity of effort, shared responsibility, partnership, and mutual support, but requires an agency with significant maritime security responsibilities to act as a coordinator for the purposes of integrating the government's efforts to provide layered security.

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

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

The Coast Guard works in concert with CBP to align respective agency roles and responsibilities regarding international trade. When cargo is moved on the waterborne leg of a trade route, the Coast Guard has oversight of the cargo's care and carriage on the vessels and within the port facility. The Coast Guard also oversees the training and identity verification of professional mariners who are transporting the cargo. CBP has authority over the cargo contents and container standards. Using the information provided through the Coast Guard's 96-hour notice of arrival rule and CBP's 24-Hour cargo loading rule, the Coast Guard and CBP act to control vessels (and their cargoes) that pose an unacceptable risk to our ports. As a further improvement, the trade community can file required passenger and crew information via an electronic notice of arrival and departure system. This streamlines the process for industry and improves our ability to apply targeting and selectivity methods. With Coast Guard officers posted at the NTC, we continuously improve agency coordination and our collective ability to quickly take appropriate action when notified of a cargo of interest.

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

Our remarks will focus primarily on how these complimentary layers enhance seaport security, and protect the nation.

Vessel Security

There are approximately 11,000 U.S. vessels that that require vessel security plans (6,200 inspected vessels and 4,800 un-inspected vessels). The Coast Guard received, reviewed and approved all domestic vessel security plans.

Since July 2004 the Coast Guard has conducted 16,000 foreign flag vessel boardings for security compliance with the International Ship and Port Security

(ISPS) Code. These boardings were conducted either offshore or in port depending on the risk assessment completed prior to each vessel arrival in U.S port. From those 16,000 boardings the Coast Guard has imposed 143 detentions, expulsions or denials of entry for vessels that failed to comply with international security requirements.

In addition the Coast Guard has established a process to identify and target High Interest Vessels. This process has resulted in 3,400 at sea security boardings and 1,500 positive vessel control escorts since 2004 to ensure these vessels cannot be used as weapons of mass effect.

Advance Electronic Information

As a result of the 24-Hour rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air, and sea, so that we know who and what is coming before it arrives in the United States. 24-Hour Advanced Cargo Rule, requiring all sea carriers, with the exception of bulk carriers and approved break-bulk cargo, to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States. However, bulk carriers are not exempt from all advance electronic information requirements—they are required to transmit cargo information 24 hours prior to arrival in the U.S. for voyages that exceed 24 hours sailing time from the foreign port of loading, or transmit at the time of departure to the U.S. for voyages less than 24 hours sailing time to the U.S. from the foreign port of loading. Failure to meet the 24-Hour Advanced Cargo Rule results in a "do not load" message and other penalties. This program gives CBP greater awareness of what is being loaded onto ships bound for the United States and the advance information enables CBP to evaluate the terrorist risk from sea containers on 100% of shipments.

In addition, the Coast Guard has taken multiple steps to enhance awareness in the maritime domain. One major step was the publication of the 96-hour Advanced Notice of Arrival regulations which requires vessels to provide detailed information to the Coast Guard 96-hours before a vessel arrives at a U.S. port from foreign ports. This regulation provides sufficient time to vet the crew, passengers, cargo and vessel information of all vessels prior to entering the U.S. from foreign ports By merging CBP and CG vessel and people information requirements into the electronic notice of arrival and departure, the reporting burden on the maritime industry will be reduced. Because the system was made available to the public on January 31, 2005, it afforded vessel owners and operators the time to become familiar with the electronic notice of arrival and departure, and consequently have an easier time complying with CBPs APIS regulation which mandated the use of this system by June 6, 2005, as the approved method for submission in accordance with the APIS regulation.

Automated Targeting System

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

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

The National Targeting Center, working closely with the Coast Guard, also vets and risk scores all cargo and cruise-ship passengers and crew prior to arrival. This ensures that DHS has full port security awareness for international maritime activity.

Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C–TPAT): Extending our Zone of Security Outward—Partnering with Other Countries

Every day, approximately 31,000 seagoing containers arrive at our nation's seaports equating to nearly 11.3 million a year. About 90% of the world's manufactured goods move by container, much of it stacked many stories high on huge transport ships. Each year, two hundred million cargo containers are transported between the world's seaports, constituting the most critical component of global trade.

All trading nations depend on containerized shipping. Of all incoming trade to the United States, nearly half arrives by ship, and much of that is in sea containers.

Other countries are even more dependent on sea container traffic, such as the U.K., Japan and Singapore.

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

If even a single container were to be exploited by terrorists, the disruption to trade and national economies would be enormous. In May 2002, the Brookings Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could amount to $1 trillion from the resulting economic slump and changes in our ability to trade.

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

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

The Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT) initiatives bolster port security. The CSI initiative proposes a security regime to ensure that all containers posing a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CBP continues to station multidisciplinary teams of U.S. officers from both CBP and Immigration and Customs Enforcement to work together with our host foreign government counterparts to develop additional investigative leads related to the terrorist threat to cargo destined to the United States.

Through CSI, CBP works 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 United States. CSI is currently operational at 43 foreign ports. By the end of 2006, we expect that 50 ports, covering 82% of maritime containerized cargo shipped to the U.S., and by the end of 2007, we expect to be operational in 58 ports covering 85% of maritime containerized cargo destined to the United States.

As directed by MTSA, the International Port Security Program has begun visiting foreign countries to assess the effectiveness of anti-terrorism measures in foreign ports.

To date, 45 countries have been assessed; 40 have been found to be in substantial compliance with the International Ship and Port Facility Security (ISPS) Code. These 45 countries are responsible for over 80% of the vessel arrivals to the United States. The five countries that are not in substantial compliance have been or will soon be notified to take corrective actions or risk being placed on a Port Security Advisory and have Conditions of Entry imposed on vessels arriving from their ports.

The Coast Guard is on track to assess approximately 36 countries per year, with a goal of visiting all of our maritime trading partners within four years

Through C–TPAT, CBP establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the United States. C–TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

C–TPAT's criteria also address physical access controls, facility security, information technology security, container security, security awareness and training, personnel screening, and important business partner requirements. These business partner requirements oblige C–TPAT members to conduct business with other C–TPAT members who have committed to the same enhanced security requirements established by the C–TPAT program.

The C–TPAT program has created a public-private and international partnership with nearly 5,800 businesses (over 10,000 have applied), including most of the largest U.S. importers. Forth-five percent of all merchandise imported into the United States is done so by C–TPAT member importers. C–TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security. CBP reviews the security practices of not only the company shipping the goods, but also the companies that provided them with any services.

The validation process employed by CBP demonstrates and confirms the effectiveness, efficiency and accuracy of a C–TPAT certified member's supply chain security.

At present, the C–TPAT program has completed validations on 27 percent (1,545 validations completed) of the certified membership, up from 8 percent (403 validations completed) a year ago. Additionally, validations are in progress on another 39 percent (2,262 in progress) of certified members, and these validations will be completed throughout 2006, bringing the total percentage of certified members to 65 percent by years' end. In 2007, the C–TPAT program validations will continue. And we will have validated 100 percent by the end of CY 2007.

Additionally, CBP has moved to tighten minimum-security criteria for membership in this voluntary program. Working closely with the trade community and key stakeholders, CBP has developed and implemented baseline security standards for member importers, sea carriers, and highway carriers. CBP will complete this process by the end of CY 2006, defining the minimum-security criteria for the remaining enrollment sectors—air carriers, rail carriers, brokers, freight forwarders, and foreign manufacturers.

The Coast Guard supports several DHS initiatives such as Operation Safe Commerce (OSC), the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C–TPAT) to ensure mutual policies, programs and initiatives are complementary and cover the entire supply chain. The CSI and C–TPAT are programs that are designed to extend supply chain security improvements to overseas ports and further along the international supply chain.

Non-Intrusive Inspection Equipment and Radiation Detection Portals:

CBP also uses cutting-edge technology, including large-scale X-ray and gamma ray machines and radiation detection devices to screen cargo. Presently, CBP operates over 680 radiation portal monitors at our nation's ports, including 181 radiation portal monitors at seaports allowing us to scan 37 percent of arriving international cargo, and that number will continue to grow through the remainder of this year and 2007. CBP also utilizes over 170 large-scale non-intrusive inspection devices to examine cargo and has issued 12,400 hand-held radiation detection devices to its CBP officers.

Further, the DHS Domestic Nuclear Detection Office's (DNDO) FY 2007 budget request of nearly $536 million, a 70% increase from FY 2006, includes $157 million that will allow for the acquisition and deployment of nearly 300 current and next-generation radiation detection systems at our ports of entry. These funds, and funds provided in FY 2005 and FY 2006, will allow for the deployment of 621 RMPs to our Nation's top seaports, which will allow us to screen approximately 98 percent inbound containers by December 2007. These systems will be deployed and operated by CBP. In addition, DNDO's FY 2007 budget also includes $30.3 million for the development of enhanced cargo radiography screening systems for our ports of entry. These enhanced screening efforts will compliment the many information-based programs CBP already has in place for enhanced port security.

In addition to increased screening efforts at our own ports of entry for radioactive and nuclear materials, the Department fully endorses the concept of increased active and passive detection at foreign ports of departure. The systems DNDO is acquiring and developing can also be used by foreign ports with a CSI presence, as well as the Department of Energy's Megaports initiative. We must continue to stress the need for increased screening at foreign ports of departure while at the same time having a robust screening effort at our own ports of entry.

Port Security Grant Program and the Coast Guard

The Port Security Grant Program is administered by the Office of Grants & Training (OG&T) in the Preparedness Directorate of DHS. The Coast Guard continues to plays an active role in the Port Security Grant Program, as it has in the first five rounds, and participates in the development of program guidance, conducts the field review process and is a member of the national review panel.

In round five of the Port Security Grant Program, $142 million was awarded for 132 projects. The current program has been improved substantially by using a risk-based formula to ensure that the projects funded provide the greatest risk reduction at the most critical ports. This same risk based formula will be used for round six in 2006.

Transportation Worker Identification Credential (TWIC)

The TWIC program, which will satisfy the requirements in MTSA under 46 U.S.C. § 47105, will ensure that only properly cleared and authorized personnel could gain access to secure areas of the Nation's transportation system.

The goals of the TWIC program are to:

• Develop a common, secure biometric credential and standards that are interoperable across transportation modes and compatible with existing independent access control systems;

• Establish processes to verify the identity of each TWIC applicant, complete a security threat assessment on the identified applicant, and positively link the issued credential to that applicant; and
• Quickly revoke card holder privileges for individuals who are issued a TWIC but are subsequently determined to pose a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards from the system.

Encompassed within the TWIC program are requirements established by the Maritime Transportation Security Act of 2002 to prevent unaccompanied individuals from entering a secure area of a vessel or facility unless the individual holds a transportation security card. Additionally, the Act requires that all holders of Merchant Mariner Credentials obtain a TWIC. With MTSA as their guide, the Coast Guard and TSA have worked closely to develop the maritime component of TWIC and are currently preparing a joint Notice of Proposed Rulemaking (NPRM).

The Coast Guard is working very closely with the TSA to assist in the implementation of this new credentialing program. The Coast Guard is supportive of this regulatory effort. We will do everything within our ability to assist TSA in the development of this rulemaking and ensure that the TWIC and Merchant Mariner Credentialing initiatives are complementary in order to minimize the burden on mariners in the future.

Post TSI Coordination

National Response Options Matrix

The National Response Options Matrix (NROM) is intended to aid crisis action decision making at the national level, immediately following a maritime transportation security incident (TSI). It does not apply to the port experiencing the TSI, however. The NROM's goal is to provide senior leadership with immediate preplanned short-term security options to prevent further attacks and protect the marine transportation system, maritime critical infrastructure and key assets (MCI/KA), and high density population centers, following a maritime TSI. NROM is a "Quick Reaction Card" decision aid for use by senior leadership to direct a possible Coast Guard wide security posture that may significantly impact maritime industry, change the maritime security (MARSEC) level, and perhaps affect/involve other DHS agencies or departments. These options may include changes in MARSEC level (for Coast Guard forces and maritime industry), potential change(s) in Coast Guard force protection condition (FPCON), or other risk mitigation options on a national level, regionally, or by specific ports. NROM has scenario-based mitigation options that were designed to build upon and strengthen existing measures, surge resources as necessary, control or restrict certain port activity, and only if necessary, close ports. NROM could also be useful in evaluating the Coast Guard's response, if any, to U. S. or world-wide terrorist incidents outside of the maritime environment.

If a maritime TSI should occur in one of our ports, the local responders (Federal Maritime Security Coordinator (Coast Guard Sector or Captain of the Port), other Federal agencies, state and local authorities, and partners in industry) will immediately react with prevention, protection, mitigation, response, and recovery activities in that port and region. The premise of NROM is to have pre-planned security options that would be put in place in other ports throughout the country to prevent and protect against further attacks. The NROM is reflected in our planning for post-incident maritime infrastructure recovery activities under the National Strategy for Maritime Security that was approved by the President last year.

NROM answers the question, "What is being done in the other ports to prevent further attacks, protect maritime infrastructure and population centers, while facilitating the continued flow of commerce and legitimate use of the maritime environment." Currently, the Coast Guard is working with CBP to incorporate CBP's response/recovery measures, making it a joint-agency decision matrix document. We have also developed an electronic NROM to improve the visibility of the product and help facilitate its use.

III. *Conclusion*

In summary, as noted already, the Coast Guard, CBP, industry partners, and many other Federal, state and local agencies work hand in hand to screen cargo, the vessels that transport the cargo and the facilities that load and discharge cargo to mitigate the risk to the Marine Transportation System. All containers and vessels that CBP and the Coast Guard determine to be of risk are examined using a variety of technologies, either at the foreign port, at sea, or upon arrival into the U.S.

Mr. Chairman, Members of the Subcommittee, we have briefly addressed DHS's critical initiatives today that will help us protect America against terrorists and the instruments of terror, while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. We realize there is more to do, and with the continued support of the President,

and the Congress, DHS will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate shipments and travelers.

Mr. LUNGREN. Thank you very much, Mr. Ahern.

And now the chair would recognize Captain Brian Salerno.

STATEMENT OF BRIAN SALERNO, DEPUTY DIRECTOR, INSPECTIONS AND COMPLIANCE, UNITED STATES COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Captain SALERNO. Good morning, Mr. Chairman, Representative Sanchez, members of the subcommittee.

I am Captain Brian Salerno, deputy director of inspections and compliance within the Coast Guard's office of the assistant commandant for prevention. It is a pleasure to be here and represent the Coast Guard, together with our colleague, Assistant Commission Ahern, to discuss some of the Department of Homeland Security's programs that are fundamental to securing our nation's ports and maintaining the economic viability of the marine transportation system.

As the federal agency responsible for maritime security in our nation's ports and waterways, we work very closely with other agencies to pursue our collective strategy of layered defense. By that, I mean a strategy that incorporates a suite of protective measures, some of which are conducted overseas, others of which are carried out on ships that are due to arrive off our shores, and ultimately with measures that are undertaken in U.S. ports themselves. I would like to take just a minute or two to put that into context.

The Coast Guard has a program established under the Maritime Transportation Security Act, commonly referred to as MTSA, to visit foreign ports and assess the degree to which they are complying with the security measures established by the International Ship and Port Facility Security Code, which is also commonly referred to as ISPFSC. ISPFSC is the international counterpart of MTSA. I am sorry about the acronyms.

To date, we have visited over 45 foreign countries. When we find ports that do not comply with ISPFSC, vessels which call at those ports, and which subsequently come to the United States, are subject to elevated levels of security. In conducting these overseas visits, the Coast Guard works very closely with Customs and Border Protection, which also assesses foreign ports as part of its container security initiative. We exchange information on foreign ports and strive to conduct our respective assessments jointly.

While in transit, ships are required to submit an advance notice of arrival. As you may recall, this was increased from a 24-hour advance notice to a 96-hour advance notice following the 9/11 attacks. The additional time allows for more thorough screening of crewmembers and passengers against terrorist watch lists, as well as giving us the opportunity to begin an initial screening of the cargo on board. The information received by the Coast Guard is shared with Customs and Border Protection as part of this initial screening process.

Based on the vessel's history and the results of our initial screening, the vessel may be subject to additional controls upon approach-

ing our shores, or if permitted to do so, upon entering our ports. Since July, 2004, the Coast Guard has conducted approximately 16,000 foreign-flag vessel boardings. These were conducted either off-shore or in port, depending upon the risk assessment completed prior to port arrival.

Since the ISPFSC code came into effect in July of 2004, the Coast Guard has imposed 143 control actions, meaning vessel detentions in port, expulsions from port, or denials of entry on vessels for failure to comply with international standards. Within the ports themselves, facilities are also subject to MTSA and ISPFSC. There are over 3,000 marine cargo facilities in the United States and each has been required to develop a security plan and submit that plan to the Coast Guard for approval.

As part of its regulatory compliance responsibilities, the Coast Guard has required corrective actions on more than 700 violations of the MTSA security regulations. Of these, 44 were severe enough to result in major control actions by the Coast Guard such as termination of cargo operations or closure of the facility until corrective measures have been taken.

One point that I do wish to make is that although the Coast Guard has an overall responsibility for enforcing security provisions of MTSA, we do not maintain a full-time presence in the facilities or on foreign vessels. It is the responsibility of the facility and the vessel operator to carry out their security plan. The Coast Guard verifies that they are doing so, and we do this with periodic visits and examinations. Naturally, the Coast Guard works very hard with the private sector to ensure that MTSA and ISPFSC are being complied with.

This is just a sampling of what we have done and are doing to preserve the security of our ports. Thank you for the opportunity to testify today, and I will be happy to answer any questions you may have when it is my time.

Mr. LUNGREN. Thank you very much, Captain Salerno, for your testimony.

The chair would now recognize Mr. Gene Pentimonti for his testimony. Thank you, sir.

STATEMENT OF EUGENE PENTIMONTI, SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS, MAERSK, INC.

Mr. PENTIMONTI. Thank you, Mr. Chairman and members of the subcommittee.

My name is Gene Pentimonti, and I am senior vice president for government relations at Maersk. I appreciate the opportunity to appear before the subcommittee this morning to discuss the very important issues of maritime security and particularly the security and accountability for every port act.

As you know, Maersk is one of the largest liner shipping companies in the world, serving customers all over the globe. With a fleet numbering more than 500 container vessels and about 1.4 million containers, we provide reliable and comprehensive ocean transportation services. Maersk, Incorporated is the North America agent for the parent company, A.P. Moller–Maersk Group's liner businesses, Maersk Line and Safmarine.

The A.P. Moller–Maersk Group employs more than 70,000 people in over 125 countries. In 1943, Maersk, Inc. was established as the general agent for A.P. Moller's liner business, Maersk Line. Here in the United States, we generate employment for approximately 12,000 Americans and we have committed to significant infrastructure investments both before and after 9/11.

Maersk has been actively involved in maritime security issues for many years. Our commitment to security is captured by the watchwords for our whole activity: constant care. The security of our containers and the integrity of our transportation network are essential to our operations at Maersk. Marine transportation is a worldwide industry and is inherently intermodal. A container that is loaded at the U.S. seaport today can be almost anywhere in the nation within a few days. For many years, cargo moved fluidly through our ports and facilities subject to prevailing regulations, but the events of September 11 changed the way we think about maritime security.

Maersk Line and all the other carriers serving the United States today are more concerned than ever about the security threats, for we know that terrorist elements might seize upon our transportation mode as an attack opportunity. To counter the potential impact on our fellow citizens, employees, port facilities, containers and vessels, Maersk has embarked on an even more aggressive enterprising campaign. We have entered voluntarily into a variety of U.S. government programs and pilot projects. For example we were the first enterprise-wide transportation company to be validated by the C–TPAT program.

We also participate in the Supercarrier Initiative program, one of only 27 ocean carriers worldwide permitted by CBP to participate at this level. But we realize that it is not enough to make our operations within this country secure, so we have intensified our efforts to secure our international cargo network through the establishment of a comprehensive and vigorous global security policy and strategy that governs our sea and land-size operations worldwide.

There is much in the SAFE Port Act that we at Maersk support and we commend you, Mr. Chairman, and other members, for working hard on maritime security. Maersk strongly supports the concept of performing the inspection functions at foreign ports before any container is loaded onto one of our vessels. We recognized that there are issues involving how this requirement can be implemented, and we pledge to work cooperatively with the U.S. and the foreign governments to achieve this desirable result.

We believe there is great promise in non-intrusive inspection and it is important that this program be developed and implemented properly. In this regard, let me state that it is essential that sufficient funding be provided to enable CBP to carry out its responsibilities on foreign port inspections. The system requires that images from screening be reviewed by CBP and that terminal operators in foreign ports receive feedback from CBP. To accomplish this, the CBP's databases need to be updated and designed so that images can be matched in real-time with information on file from CBP. Then in cases where further inspections are required, the additional inspection can occur immediately.

Furthermore, for inspections in foreign countries to succeed, it must either be accomplished through bilateral or multilateral negotiations between the United States and countries where the requirements are imposed, or we must provide incentives for foreign port operators to perform those functions. The SAFE Port Act contains provisions appropriately addressing high-risk containers that can be identified before they reach American soil.

A very significant part of this discussion about mechanisms to improve maritime security is the vessel cargo manifest. This manifest, based on longstanding regulatory and commercial standards, provides a great deal of specific useful information on all cargo that is brought into the United States. Among other items, it identifies the contents of the container or the cargo carried on board the vessel; the identity of the shipper and consignee; the port of origin; and the destination within the United States.

We concur strongly with the provisions in the SAFE Port Act that enhanced manifest information is needed. It is the responsibility of shippers who possess this information to provide it and we must protect them and their confidentiality and integrity of the data.

Of course, we also must be certain that the right kind of information is collected, as ocean carriers do not have, nor is there a need to have, this type of information. We must also be sure that the information collected can be acted upon quickly and that this process does not introduce an unreasonable amount of friction into the flow of global trade.

Section 8 of the SAFE Port Act addresses the issue of employee identification. As you know, the MTSA Act of 2002 mandated that government develop this and issue credentials, including biometric identifiers and background checks, for transportation workers seeking unescorted access to secure areas within transportation facilities. We support the concept of the TWIC and pledge to provide information to assist in improving employee identification and assist in the implementation of the TWIC program.

We are still in the process of examining thoroughly the SAFE Port Act, but please permit me to offer several general observations at this time. We will, of course, continue to discuss with you the specific issues that may arise through our review. A number of requirements are imposed by the SAFE Port Act and they must be evaluated with an eye toward reciprocity and their application to both imports and exports. We must anticipate whether our foreign trade partners will impose similar requirements and whether it is feasible for U.S. interests to comply.

The SAFE Port Act or any other maritime security legislation should not duplicate or conflict with other requirements of law, and not add unnecessary levels of bureaucracy. Security is already a very complicated area and additional levels of paperwork and involvement by multiple agencies will not further the goal of making our marine transportation system safer.

We support the continuation of C–TPAT and strongly believe the program should remain voluntary and not subject to governmental rulemaking. C–TPAT should be flexible enough to permit variations in the application to participants and not impose a generic set of rules on all of them.

If a program similar to GreenLane is adopted, it must provide clear, direct benefits in return for implementing high security standards. This is essential if companies are going to undertake investments needed to become involved in the program and make the change the program requires. Today, the MTSA already requires the Department of Homeland Security to set standards for container security devices. CBP and DHS are testing devices against these standards. We should await the outcome of these tests and determine their technological feasibility before proceeding on this matter.

Mr. Chairman, Maersk works hard to make our operations as safe as possible. This is in the national security interests of our country, our own commercial interests, and the interests of providing a safe and secure workplace for the environment of our employees. We at Maersk look forward to continuing discussing the SAFE Port Act and other security issues with you. I am happy to answer any questions that you may have.

Thank you very much.

[The statement of Mr. Pentimonti follows:]

PREPARED STATEMENT OF EUGENE K. PENTIMONTI

Mr. Chairman, my name is Gene Pentimonti, and I am Senior Vice President for Government Relations at Maersk. I appreciate the opportunity to appear before the Subcommittee this morning to discuss the very important issue of maritime security and, in particular, the Security and Accountability for Every (SAFE) Port Act.

As you may know, Maersk is one of the largest liner shipping companies in the world, serving customers all over the globe. With a fleet numbering more than 500 container vessels and about 1.4 million operated containers, we provide reliable and comprehensive ocean shipping transportation. Maersk, Incorporated is the North America agent for parent company A.P. Moller-Maersk Group's liner businesses, Maersk Line and Safmarine. The A.P. Moller-Maersk Group employs more than 70,000 people in over 125 countries.

In 1943, Maersk, Inc. was established as the general agent for A.P. Moller's liner business, Maersk Line. Here in the United States, we generate employment for approximately 12,000 Americans and we have committed to significant infrastructure investments before and since September 11, 2001.

Maersk has been actively involved in maritime security issues for many years. Our commitment to security is captured by the watch words for all our activities: "Constant Care." The security of our containers and the integrity of our transportation network are essential to our operations at Maersk. Marine transportation is a worldwide industry, and it is inherently intermodal—a container that is unloaded at a U.S. seaport today can be almost anywhere in the nation tomorrow or within days.

For many years, cargo moved fluidly through our ports and facilities subject to prevailing regulations. But the events of September 11, 2001 changed the way we think about maritime security. Maersk Line and other carriers serving the United States today are more concerned than ever about security threats, for we know that terrorist elements might seize upon our transportation mode as an attack opportunity.

To counter the potential impact on our fellow citizens, employees, ports facilities, containers and vessels, Maersk has embarked on an even more aggressive, enterprising campaign. We have entered voluntarily into a variety of U.S. government programs and pilot projects—for example, we were the first enterprise-wide transportation company to be validated by the Customs-Trade Partnership Against Terrorism (C–TPAT) Program. We also participate in the Super Carrier Initiative Program, one of only 27 ocean carriers worldwide permitted by U.S. Customs and Border Protection (CBP) to participate at this level. But we realize that it is not enough to make our operations within this country secure, so we have intensified our efforts to secure our international cargo network through the establishment of a comprehensive and vigorous global security policy and strategy that governs our sea and landside operations worldwide.

There is much in the SAFE Port Act that we at Maersk support and we commend you, Mr. Chairman, and other Members for working hard on maritime security.

Maersk strongly supports the concept of performing the inspection function at foreign ports—before any container is loaded on a vessel. We recognize that there are issues involving how this requirement can be implemented, and we pledge to work cooperatively with U.S. and foreign governments to achieve this desirable result. We believe there is great promise in non-intrusive inspection and it is important that the program be developed and implemented properly.

In this regard, let me state that it is essential that sufficient funding be provided to enable CBP to carry out its responsibilities of foreign port inspections. The system requires that images from screening be reviewed by CBP and that terminal operators in foreign ports receive feedback from CBP. To accomplish this, the CBP's databases need to be updated and designed so that images can be matched in real time with information on file with CBP. Then, in cases where further inspection is required, the additional inspection can occur immediately.

Furthermore, for inspections in foreign countries to succeed, it must either be accomplished through bilateral or multilateral negotiations between the United States and countries where the requirements are imposed (with the foreign country implementing the security procedures), or we must provide incentives for foreign port operators to perform those functions.

The SAFE Port Act contains provisions appropriately addressing high-risk containers that can be identified before they reach American soil. A very significant part of the discussion about mechanisms to improve maritime security is the vessel cargo manifest. This manifest, based on long standing regulatory and commercial standards, provides a great deal of specific, useful information on all cargo that is brought into the United States. Among other items, it identifies the contents of the container or the cargo carried onboard the vessel, the identity of the shipper and consignee, the port of origin, and the destination within the United States. We concur strongly with provisions in the SAFE Port Act that enhanced manifest information is needed. It is the responsibility of shippers who possess this information to provide it and we must protect the confidentiality and integrity of the data. Of course, we also must be certain that the right kind of information is collected as ocean carriers do not have—nor is there a need to have—this type of information. We must also be sure that the information collected can be acted upon quickly, and that this process does not introduce an unreasonable amount of friction into the flow of global trade.

Section 8 of the SAFE Port Act addresses the issue of employee identification. As you know, the Maritime Transportation Security Act of 2002 (MTSA) mandated that the government develop and issue credentials (including biometric identifiers and background checks) for transportation workers seeking unescorted access to secure areas within transportation facilities. We support the concept of the Transportation Worker Identification Card (TWIC), and pledge to provide information to assist in improving employee identification and assist in the implementation of the TWIC program.

We are still in the process of examining thoroughly the SAFE Port Act, but please permit me to offer several general observations at this time. We will of course continue to discuss with you specific issues that may arise through our review.

- A number of requirements are imposed by the SAFE Port Act, and they must be evaluated with an eye toward trade reciprocity, and their application to both imports and exports. We must anticipate whether our foreign trade partners will impose similar requirements, and whether it is feasible for U.S. interests to comply.
- The SAFE Port Act or any other maritime security legislation should not duplicate or conflict with other requirements of law, and not add unnecessary levels of bureaucracy. Security is already a very complicated area, and additional levels of paperwork and involvement by multiple agencies will not further the overall goal of making our marine transportation system safer.
- We support the continuation of C–TPAT, and strongly believe that the program should remain voluntary and not subject to governmental rulemaking. C–TPAT should be flexible enough to permit variations in its application to participants, and not impose a generic set of rules on all of them.
- If a program similar to GreenLane is adopted, it must provide clear, direct benefits in return for implementing high security standards. This is essential if companies are going to undertake the investment needed to become involved in the program and make the changes the program requires.
- Today, the MTSA already requires that the Department of Homeland Security (DHS) set standards for container security devices, and CBP and DHS are testing devices against these standards. We should await the outcome of these

tests and determine their technological feasibility before proceeding on this matter.

Mr. Chairman, Maersk works hard to make our operations as safe as possible. This is in the national security interests of our country, our own commercial interests, and the interests of providing a safe and secure workplace environment for our employees. "Constant Care" are our watchwords, and they form the foundation of every activity we take in this regard.

We at Maersk look forward to continuing to discuss the SAFE Port Act and other security issues with you. I am happy to attempt to answer any questions you may have, and I appreciate very much the opportunity to appear before you this morning.

Mr. LUNGREN. Thank you, Mr. Pentimonti, for your testimony.

The chair would now recognize Mr. Noel Cunningham.

STATEMENT OF NOEL CUNNINGHAM, PRINCIPAL, MARSEC GROUP

Mr. CUNNINGHAM. Mr. Chairman and members of the committee, thank you for inviting me to testify before you today. I will be addressing the proposed Security and Accountability for Every Port Act, or SAFE Port Act. During this testimony, I will address the act and discuss other actions I believe are critical in addressing the vulnerabilities associated with maritime security.

My assessment is based upon my 40 years of experience as a law enforcement officer, chief of the Port of Los Angeles Police, and director of operations at the nation's largest seaport. In the interests of time, I would like to summarize my testimony and submit a complete written copy to the committee. I should also note that this testimony was prepared with the assistance of two other principals for the MARSEC group, Captain John Holmes, former captain of the Port of Los Angeles–Long Beach, and Dr. Charles Massey, who retired recently from Sandia National Laboratories as the program manager for the Department of Energy's Second Line of Defense.

As you may be aware, Captain Holmes and Dr. Massey have significant experience in port and border security and like myself were in the field during and after the tragic events of September 11. Having had the opportunity to review the SAFE Port Act, I would like to commend the committee for its efforts and go on record as supporting the concepts embraced in the act. I wholeheartedly support the efforts outlined in areas of strategic planning, information management, and data integration.

I am also pleased to see that the bill addresses existing concerns regarding trade reconstitution, that it will better define the GreenLane concept, and that it embraces the use of a common metric in the grant process.

My experience leads me to believe, however, that the act could be made significantly more effective if this committee expanded its scope in order to establish new priorities for existing programs that are critical to the security of our ports. These include port identification, enhanced inspections in foreign ports, and security system integration at the local ports, regional and the national levels.

I am also encouraged to see that the bill addresses the critical issue of research and development. It is my strong belief that our focus needs to transcend our current efforts at plugging the security gaps that we know, and embrace identification and prevention of those that we currently do not know about. If this is going to

be done, intelligence gathering and research and development will be key elements in the success of these efforts.

Although I am heartened by the areas of focus, I would like to see it expanded to specifically embrace all methods of cargo screening, including those that have proven to be most problematic up to this point: biological and chemical detection. Although I recognize this issue is generally addressed in some of the existing regulations, I would also like to support the idea of establishing requirements for training and exercises in the bill. As a career law enforcement officer, I cannot underscore enough the importance of a solid training program.

It is my belief that when an assessment is conducted, key gaps will be identified. Three of these include inability to clearly determine who is working on our ports. Unlike our airports, our seaports have no credentialing program. One of the universal truths in law enforcement is that security starts with people. Responsible citizens are oftentimes much more reliable and accurate in detecting and deterring criminal or terrorist activity than sophisticated technological systems, just as Congresswoman Harman identified for the ILWU. If bad people cannot undertake their efforts without being exposed, the system will be more secure.

Number two, inability to truly know what is in the containers that are arriving in the U.S. As my close friend and colleague Dr. Stephen Flynn has stated, the question must be asked: What is in the box? Given the complexity of the supply chain and the number of individuals involved, the only means to truly assure that the contents of the container do not pose a threat is to use technology to screen the contents. No port chief or captain of a port wants to be the individual who finds the dirty bomb after he has off-loaded it in his or her port.

Third, lack of integration of current security systems on the local port, regional and national levels. In the post–9/11 climate, ports and terminals have embraced the use of security systems, cameras, access control and intrusion detection systems. Unfortunately, there are very few cases where ports have taken the lead and have found the funding to integrate these systems. As a result, knowledge of security breaches or attempted breaches are only known to that particular system.

The gaps identified represent fundamental security shortfalls that must be addressed. Access control and overseas screening are the foundations to secure our supply chain and they represent the most significant and most efficient means to push back the borders. Until shortfalls such as these are rectified, the security of the entire supply chain must be called into question.

Involvement of industry is also crucial in this effort. No one knows better where the security vulnerabilities are in the maritime industry than the industry. Tapping into this knowledge base is crucial. Operation Safe Commerce, in which me and my partners were key participants, is an example of industry helping to determine where the security efforts are best placed. The SAFE Act program continues to recognize and support this crucial industry-led effort.

While container security is rightly the subject of much focus, cargo does not only move through the maritime industry in steel

boxes. A weapon of mass destruction could also be transported to the United States on a bulk haul container, a roll on-roll off vessel, or a fishing trawler. Security of our nation depends on systems that will deal with all types of maritime threat delivery opportunities.

I am pleased to see that the focus of this bill goes beyond containerized cargo and that research, development and testing of the processes and technologies will be addressed and that prioritized threats throughout the maritime system are included in this act.

I also believe that if one is going to address the security needs, the issue of resources cannot be ignored. A question that must be asked during the planning and analysis stage outlined in this bill must be: Are the federal, state and local resources on hand sufficient to educate, deter, detect, respond and recover in the manner expected? I think that unfortunately the answer will be no.

I, more than most, realize that priorities must be established based on principles of risk management. I have lived this reality for 40 years. Unfortunately, when organizations become driven more by funding parameters than risk management principles, adjustments need to be made. This is the situation we now find ourselves in. As such, I implore you to include as part of the planning requirements in this bill a match of the mission requirements and resources needed.

I would once again like to commend the committee for your efforts. I can see that a great deal of work and thoughtful analysis has gone into this project. I am convinced that if additional concerns are addressed in areas such as port user identification, the TWIC, overseas inspections and security integration, the act has the ability to significantly enhance port and maritime and supply chain security.

I would like to offer my assistance and the assistance of my colleagues and myself to support you in any way possible. I would like to also publicly acknowledge the hard work that my Congresswoman Millender–McDonald, has put into port security bill, H.R. 478. I do know that the congresswoman desires working with this distinguished committee in considering some of the elements of H.R. 478 with the SAFE Act bill.

I thank you, and I will be happy to answer any questions you may have.

[The statement of Mr. Cunningham follows:]

PREPARED STATEMENT OF CHIEF NOEL CUNNINGHAM

Mr. Chairman and Members of the Committee, thank you for inviting me to testify before you today. I will be discussing the proposed "*S*ecurity and *A*ccountability *F*or *E*very Port Act" or "SAFE Port Act." During this testimony I will address the act, and discuss other actions that I believe are critical in addressing vulnerabilities associated with maritime security. My assessment is based on my 40 years of experience as a law enforcement officer, Chief of the Port of Los Angeles Police, and Director of Operations at the largest port in the United States. My testimony is also being provided from my vantage point as a Principal of The Marsec Group—a small group that provides maritime and supply chain security consulting services to public and private sector clients.

I should also note that this testimony was prepared with the assistance of the two other principals from The MARSEC Group: Captain John Holmes, former Captain of the Port of Los Angeles—Long Beach and Dr. Charles Massey, who retired recently from Sandia National Laboratories as the program manager for the Department of Energy Second line of Defense Program. As you may be aware, Captain

Holmes and Doctor Massey have significant experience in port and border security, and like myself were "in the field" during and after the tragic events of September 11th.

Having had the opportunity to review the SAFE Port Act, I would like to commend the committee for its efforts, and go on record as supporting the concepts embraced in the act. I wholeheartedly support the efforts outlined in the areas of strategic planning, information management and data integration. I am pleased to see that the bill addresses existing concerns regarding trade reconstitution. I am also very encouraged by the fact that the bill will better define the GreenLane process and that it embraces the use of a common metric in the Port Security Grant process.

My experience leads me to believe, however, that the act could be made significantly more effective if this committee expanded its scope to establish new priorities for existing programs that are critical to the security of our ports. These include port user identification, enhanced inspections in foreign ports, and security system integration at the port, regional and national level.

It is clear that the purpose of the "SAFE Port Act" is to improve maritime and cargo security, thereby protecting the safety and security of our citizens, our nation, and its economy. With over 80 percent of international trade volume carried by the maritime system, the likelihood that it will be targeted in the future by terrorists should be assumed. Although a great deal of discussion has taken place regarding whether maritime shipping is an appropriate means of transportation for a weapon of mass destruction, I firmly believe that this discussion misses the mark. If one is looking for a means of transport for a WMD there may be better vehicles. If one is looking for a means to cripple our economy, the transportation system is an exceptional target.

Past terrorist attacks against an oil tanker and a LNG carrier would seem to support that the marine transportation system is both the "target" and the "arrow". To combat the terrorists and deploy systems to win the war on terror, the United States must aggressively support security programs already underway while implementing new ones to deal with the dynamic threat posed by modern day terrorists.

Although the "SAFE Port Act" proposes a set of initiatives to complement, and/or improve several existing maritime security programs, it is critical that an assessment of existing programs is conducted in order to identify and fill fundamental security gaps. The "SAFE Port Act" includes this crucial element and requires the development of a Strategic Plan to deal with the threat and ensure that security efforts are focused on the right issues. Equally important, given the likelihood of an attack on the maritime system, is an understanding of how the system will be restored after an attack. I am pleased to see that the Act addresses this important issue.

I am encouraged to see that the bill addresses the critical issue of research and development. It is my strong belief that our focus needs to transcend our current efforts at plugging the security gaps that we know, and embrace the identification and prevention of those that currently do not exist. If this is going to be done, intelligence gathering and research and development will be key elements in the success of these efforts. Although I am heartened by these areas of focus, I would like to see the Act expanded to specifically embrace all methods of cargo scanning including those that have proven to be most problematic up to this point, i.e. chemical and biological detection.

I also believe that the bill would be more comprehensive if the research and development section specifically addressed the issue of improving portable detection equipment. If we are truly going to embrace the concept of pushing back the borders and developing a multi-layered layered security system, it is critical that we not only conduct most of our inspections overseas (as is currently the focus of the Container Security and Megaports initiatives), but that we also provide our seagoing inspection teams the equipment that is needed to prevent illicit materials from being transported into and through U. S. waters. Seagoing examinations are hazardous undertakings. It is critical therefore that we develop equipment that is specifically made for the maritime environment.

Although I recognize that this issue is generally addressed in some of the existing regulations, I would also like to support the idea of outlining requirements for training and exercises in the bill. As a career law-enforcement officer I can not underscore enough the criticality of a solid training program. It is my belief that this bill should require ports and port personnel to take a leadership role in port security training. Requirements should be put in place requiring port and regional training exercises in such areas as response, personnel evacuation and reconstitution of operations.

It is my belief that when an assessment is conducted, key gaps will be identified. These include:

• Inability to clearly determine who is working in our ports: Unlike our airports, our ports have no credentialing system. One of the universal truths in law enforcement is that security starts with people. Officers and responsible citizens are oftentimes much more reliable and accurate in detecting and deterring criminal, or terrorist, activities than sophisticated technological systems. If bad people can not undertake their efforts without being exposed, the system will be more secure. Identification of workers through efforts like the Transportation Worker Identification Card (TWIC) are on target and expansion of this type of information assessment and utilization to other members of the supply chain, including shippers, carriers, freight forwarders, and creditors, as mandated by this Act will improve security. However, issues associated with the privacy of the data will need to be addressed. Through a cooperative effort involving labor, the industry, and the government, I believe the important "information" component of the maritime system—a component that would include information about the cargo and the people involved in its purchase and movement—can be used to make the system more secure. Credentialing and access control are the foundation of any effective security system. This program needs to become the highest security priority.

• Inability to truly know what is in the containers arriving in the U.S: As my close friend and colleague, Dr. Stephen Flynn has stated, the question that must be asked is "what's in the box?" Given the complexity of the supply chain and the number of individuals involved, the only means to truly ensure that the contents of the container do not pose a threat is to use technology to screen the contents. In order to truly embrace maritime security, this screening must be forced to occur prior to loading. At present the amount of foreign inspections is simply not significant enough to provide a deterrent effect. No Port Chief of Operations or Coast Guard Captain of the Port wants to be the individual who finds the dirty bomb after it is offloaded in his or her port.

• Lack of integration of current security systems on the port, regional and national level: In the post 9/11 climate ports and terminals have embraced the use of security systems that include, cameras, access control and intrusion detection systems. Unfortunately there are few cases where ports have taken the lead, and/or found the funding to integrate these systems. As a result, knowledge of security breaches or attempted breaches are not known outside the identifying system, nor are they examined systematically. What currently exists in most ports is a conglomeration of individual hardware, and not a port-wide security system.

The gaps identified represent fundamental security shortfalls that must be addressed. Access control and overseas screening are foundational to supply chain security, and they represent the most efficient means to push back the borders. Until shortfalls such as these are rectified, the security of the entire supply chain must be called into question.

While the use of information assessment tools and sophisticated detection systems by government agencies are two important legs of the three-legged security stool, system security will not be achieved unless the last leg of the stool is accounted for. This leg consists of the major players in the maritime transportation system—labor, terminal operators, shippers, carriers, and port authorities. Involvement of these stakeholders has been pursued through initiatives such as the Customs-Trade Partnership Against Terrorism (C–TPAT). I am pleased to see that the "SAFE Port Act" wisely endorses this effort.

I believe the shipping industry wants to do more in the area of security. Because they are in business, they must be able to justify some of the expense and I believe they are right to expect something in return for their investment. For example, businesses that invest in the security measures required for participation in C–TPAT should be given priority in clearing their cargo through customs over business that do not. Designation of a GreenLane with achievable and definable requirements will do much to persuade businesses to invest in processes and technologies that can make us more secure.

The involvement of industry is also crucial from another aspect. No one knows better where the security vulnerabilities are in the maritime industry than the industry. Tapping into this knowledge base is crucial for success. Operation Safe Commerce, of which my partners and I were key participants, is an example of industry helping to determine where security efforts are best placed. The "SAFE Port Act" continues to support this crucial industry-led effort.

While container security is rightly the subject of much focus, cargo does not only move through the maritime system only in steel boxes. A Weapon of Mass Destruction (WMD) could also be transported to the United States on a bulk oil tanker, a Roll-on/Roll-off vessel, or a fishing trawler. Security of our nation depends on sys-

tems that will deal with all types of maritime threat delivery vehicles and targets. I am please to see that the focus of the bill goes beyond containerized cargo and that research, development and testing of processes and technologies that will address prioritized threats throughout the maritime system, are included in this Act.

I also believe that if one is going to address security needs, the issue of resources can not be ignored. A question that must be asked during the planning and analysis required in this bill must be: "Are the federal, state and local resources on hand sufficient to educate, deter, detect, respond, and recover in the manner expected?" I think that the unfortunate answer to this question will be "no". I, more than most, realize that priorities must be established based on the principals of risk management. I have lived this reality for over 40 years.

Unfortunately, when organizations become driven more by funding parameters than risk management principals, adjustments need to be made. This is the situation we now find ourselves in. As such, I implore you to include, as part of the planning requirements in the bill, a match of the mission requirements and resources needed.

I would once again like to commend the Committee for your efforts. I can see that a great deal of work and thoughtful analysis has gone into this project. I am convinced that if additional security concerns are addressed in areas such as port user identification, overseas inspection, and security integration, the Act has the ability to significantly enhance port, maritime and supply chain security. I would like to offer the assistance of my colleagues and myself to support you in any way possible in moving this critical Act forward.

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

Mr. LUNGREN. Thank you very much, Mr. Cunningham.

The chair will recognize all members for 5 minute periods for questions. I will start the round of questions.

Mr. Ahern, you heard Mr. Cunningham say that one of the major concerns, if not the major concern, is "what is in the box." Some people have said, well, the solution is fairly simple. We have to inspect every single container in every single foreign port before it comes here.

What are we doing in that regard? Is that possible? And people keep referring to the Hong Kong experience, where they seem to be able to do this, at least I hear that repeated many, many times, that they get to look at 100 percent of all the containers and why can't we do the same.

Mr. AHERN. Thank you very much. There are several questions in there, and I will answer in order, sir.

First, when you take a look at the data elements to help us identify what is in the box, there are currently 24 elements of the manifest that we use for targeting, 17 off the entry. We are in the process right now of identifying what additional elements we do need for targeting so that we can make a better determination of what is in the box. We then run it through our automated targeting systems.

We are also looking to see what the appropriateness is of changing some of the timeframes for filing of entry information, as opposed to receiving it at or after the time of arrival. We want to move that up, so we are considering that.

We also need to take a look at the stow plan that is electronically available to make sure that we can match that against some of the information that is sent to us electronically to make sure there is no unmanifested boxes. That information is available, so we are seeing how we can introduce that into our system as well.

Overseas, we have now expanded as recently as March 8, and brought about our 43rd container security initiative port. We now

have close to a little over 74 percent of the containers coming to the United States actually transit through those overseas ports.

Your last point relative to the ICIS model that is in Hong Kong, I had the opportunity to go and look at that in October of this past year. I would say that as has been represented by many, it is completely oversold as far as what its current capability is. It has been misrepresented as to what it is currently doing. It is not doing 100 percent of the containers. It is set up in one land of one of the terminals there to just put about 300 containers an hour through there.

I will tell you that certainly the concept is a good one. We need to take a look at it. We need to take a look at how we could deploy it in a very well thought-out manner. So it does continue to provide the level of pushing the borders out screening that is necessary to have the appropriate threshold setting for alarms, with a radiation portal monitor. There needs to be a concept of operation that is meaningful, not just pushing containers through that model that is currently out there. We also need to take the opportunity to develop good, well thought-out response protocols to resolve the alarms.

We are currently in the analysis right now of some of the containers that have been put through there. We just within the last couple of weeks received 21,000 files from the computer that had been collecting some of the radiation spectra, so that we can do an analysis both with our subcontractor, which is Pacific Northwest Laboratories, and also the Department of Energy has brought in the Oakridge National Laboratory to do some analysis for us as well, so we could actually come up with a model of how many alarms would a terminal operator expect in an overseas environment that would need to be resolved prior to lading.

So to sum up on the ICIS concept, I think it is again currently been clearly overstated as far as what its current capabilities are. It is not doing 100 percent. It is principally the same technology we use here in the United States, so it is not a question about the efficacy of the technology, but it is how do we deploy the concept of operations effectively so it is a meaningful test, and we have the right protocols in place.

Mr. LUNGREN. Let me ask this, and both for Mr. Ahern and Captain Salerno. You have your plan in place. You have figured your at-risk containers and so forth. You know there has been some check on them at the foreign ports. What is to say there is not going to be someone opening the container while en route? Taking something in; putting something in; taking something out, et cetera.

Mr. AHERN. Certainly, that is a vulnerability in the supply chain and we are not dismissing that fact. We have been very aggressively with the department's Science and Technology Directorate looking at the appropriate container security devices that could help as a solution for that. We think we need to fast-forward that process.

We have taken a look at we need to have a 99.6 effectiveness rate with the device so that we are not resolving nuisance alarms, because we are looking at a universe of over 11.3 million containers

in fiscal year 2005 came into the United States from overseas. We are looking at about a 12 percent growth expected for this year.

I would not want to have our officers focusing on nuisance or false alarms because the technology is not working effectively. Our testing has currently been showing somewhere in the 94 to 96 range as far as for accuracy, and four to six points of having to resolve against a universe of 11 million containers gets into the 400,000, 500,000, 600,000 containers that need to be alarmed just because the technology is not working correctly.

So we need to continue to get better with that. We have challenged the industry to continue to fine-tune to make sure they meet our current specs, and we are looking forward to coming up with a solution, because it is absolutely a key vulnerability that needs to be sealed with an appropriate container security device.

Mr. LUNGREN. Captain Salerno?

Captain SALERNO. Yes, sir. One of the elements of the vessel security plan that is required under MTSA and under ISPFSC internationally are provisions to guard against tampering of the cargo. Essentially, this puts a burden on the ship's crew for vigilance.

What we have seen in terms of whether this works or not, we have in fact had a case where there were stowaways in a box and they did egress the box while onboard the vessel in mid-ocean. They were detected by the crew, and that situation was in fact reported to the Coast Guard. So it is just one example of how the plan in fact did work in that case.

Mr. LUNGREN. I have a lot of questions to follow up, but my time is up.

Ms. Sanchez is recognized for 5 minutes.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Again, I want to thank you all for being before us, and in particular Chief Cunningham, welcome back. I think you were my guest on the panel 2 1/2 years ago when we had this committee at the time.

Mr. Chairman, you were not in the Congress for the second time, but we had Mr. Cunningham before our committee in Los Angeles where we held one of our first hearings. He has been an incredible resource for a lot of the information that we have on many of the bills that we have introduced.

So welcome back and thank you for being with us. I certainly will continue to enjoy yours and Mr. Holmes' and others' information and expertise as we try to work through this.

My questions have to do with C–TPAT, because as you said, Chief Cunningham, what is in the box is incredibly important. Let's face it, the majority of what we do is we read the list of what somebody is telling us is in the box. That is what is going on. And in many cases, my longshoremen tell me, there are other things in the box, and we will be making a field trip tomorrow to the ports to see how advanced we have gotten since the last time we were there, the last time we saw the X-ray machine that takes a look at the container, the last time we discussed the number of manhours that it takes CBP to pull apart a container and look at everything.

Yes, I hope it has gotten better, but I really don't believe we have gotten better X-ray technology that we had last year or the year

before when we were there. I also don't believe that we are checking that many more containers that are coming in. So what is in the box?

So we have this program, C–TPAT, where we have 10,000 companies signed up to participate in it. To this point, only 1,545 of those companies have had their security measures validated. That means we ask these companies, we tell them you are going to get some benefits, you are going to go faster and get your stuff through faster, if you write us a plan that tells us all your security measures, and how you are going to make sure that your vendors are doing the right thing and everything is secure and your manifests are right, et cetera, et cetera.

And of these 10,000, we have validated, I think that is from CBP, 1,545. So there are thousands of companies that are receiving benefits despite the fact that there has been no confirmation of the security measures that are in place at these companies.

So my question is, when will all of the currently pending validations be completed? I think this is to Mr. Ahern. And I don't want to hear about possibly certified companies, because I understand that that would mean that you received it, you stamped it as received, and then you gave certification to companies.

So I want to know what is the pending validation; how long is it going to take you to get these 10,000 companies done; and aren't you granting risk or reductions to companies whose security plans have not yet been really been checked?

Mr. AHERN. I would be happy to provide you with a full answer on that. Of the 10,000 applicants, and we have 5,800 certified members. That is the appropriate universe to apply these credits for the risk scoring as well as for the validations.

Ms. SANCHEZ. So what does "certified" mean?

Mr. AHERN. "Certified" means that they have actually supplied a security assessment to us that we have reviewed, and we have gone back and forth with the company in many iterations to make sure it is an appropriate security plan where they can demonstrate through their written submitted security plan of what they are doing overseas. They are not receiving any credit at that point until the plan is actually initially certified.

Ms. SANCHEZ. Wait. So if you are initially certified, you haven't gone to really see what is going on. You have just taken their plan, you have reviewed it with them, and then you have certified it.

Mr. AHERN. That is correct.

Ms. SANCHEZ. And now you are giving them credit scores for being good companies.

Mr. AHERN. Partial credit. We have it in three tiers. That would be the first credit they would receive some benefit for. We then have the universe of those that then are certified and validated. We currently have, as you stated, 1,545 companies which represents 27 percent of the universe of 5,800 certified members that are actually validated at this point. We have another 2,262 validations currently in progress which would bring us up to 39 additional percent.

So our goal is to be at 65 percent completed by the end of this calendar year. I am not happy where our progress has been. We had a total authorized level of 157 supply chain security specialists

to hire this year. We are currently only in the mid–80s as far as with the current onboard strength. We just made a recent selection of 40 individuals that should be onboard within the next 30 to 45 days, so we should have an opportunity to get those numbers significantly more accomplished in the coming months.

Ms. SANCHEZ. So you have 80 people to check 10,000 companies?

Mr. AHERN. We have currently 80 supply chain security specialists that are doing the validations. We have 40 more that are currently in the final review for EOD-ing within the next 30 to 45 days.

Ms. SANCHEZ. I have a lot more questions, as you can tell, Mr. Chairman, but I will yield back and hopefully you will give us another round.

Mr. LUNGREN. Yes, we shall.

Ms. Harman is recognized for 5 minutes.

Ms. HARMAN. Thank you, Mr. Chairman. Again, thank you and the ranking member for allowing me to participate in the subcommittee.

I do want to say that I think your visit tomorrow to the ports of L.A. and Long Beach will be excellent. I apologize that I will not be there. I have a date with a new granddaughter and she lives in New York City, so I am going to Los Angeles via New York City. My apologies.

I thought your testimony was excellent. I think there is a lot of information on the record now about the very good things that are happening. Our ports are more secure than they were on 9/11. Again, I want to thank the Coast Guard in particular for heroic efforts.

We have something in this bill about joint operations centers, which we intend to be the place that would take charge in an emergency. I have often heard the comment that it is not clear who is in charge. I do want to ask all of the witnesses about your views of these joint operations centers and whether you think they will be useful and whether they will add to, not compete with, the excellent capability we already have on the ground.

Just before you answer, because I am thinking my time will run out, I do want to commend something that we have in Los Angeles, which is the Area Maritime Security Committee, which does integrate all levels of government and does include I believe the private sector as well, and is by my lights a very important improvement since 9/11.

I was recently there accompanied by Senator Susan Collins. We were there to ask the question: Are we ready for a major terrorist attack? Obviously, the answer is no one can be totally ready, but surely in the ports of L.A. and Long Beach we have a very significant prevention and response capability. So I want to commend you, and if you want to say anything about the state of readiness as you answer my question about the need for a joint operations center, please do that.

This is to all the witnesses.

Mr. CUNNINGHAM. I will respond that Los Angeles is the point that you identified as one of those models that you are pleased with. I, too, am pleased with the model. We have received exceptional leadership with the Coast Guard, the leadership of the Coast

Guard and the captain of the port has been very strong in promoting the Area Maritime Security Committee, which is mandated by the Maritime Transportation Security Act.

What makes the model work, though, it is an operation that involves all of the stakeholders. We have labor, we have the terminal operators, we have the local law enforcement, we have the federal agencies, the regulatory agencies. From that standpoint, yes, we do need it, and that language should stay in the bill. It is very important, and also I would suggest that we add exercises. The training and the exercises make that bill work. Right now, there is no mandate for that, but it is just the pure leadership that we are getting out of the Coast Guard that is making that work.

Ms. HARMAN. Let me second your comment about the training and the exercises, but they also need to be, as I learned at that meeting a few weeks ago, really targeted in a better way than they are. And they need to be repetitive. We can't do just one big bang, get a headline in a newspaper, and figure that the workforce and all of the stakeholders are adequately trained. Do you agree?

Mr. CUNNINGHAM. I do agree. To not have the continuous and the repetition of the training, you have changes, the Coast Guard will change their leadership and their decision-makers and so will the local authorities. So it is important to have this training as part of the fabric of your security program and the change does not impact the leadership or change of the rules.

Ms. HARMAN. Mr. Chairman, I will be quiet. But could the other witnesses answer my question? Can we accommodate that? Thank you.

Captain SALERNO. Good morning, Congresswoman.

I would like to address the command center concept, because it is a very important one for the Coast Guard. As you may know, the Coast Guard has reorganized its field infrastructure where we had previously marine safety officers and group commands, they have been merged into what we now call sectors. There are 35 sectors established around the country. Essentially every port area in the nation is under the jurisdiction of at least one sector.

Every sector has a command center. Part of their mandate is to engage local partners, other federal, state and local law enforcement, as well as private sector, port authorities and such. You mentioned the Area Maritime Security Committees, that is a requirement of the Maritime Transportation Security Act, so that in every Coast Guard area of operation, there is an Area Maritime Security Committee which brings together all of these stakeholders in the port community. Collectively, they are responsible for generating an area maritime security plan.

We have authority and have exercised the authority to give certain members of this marine community, outside of the law enforcement community and outside the federal government, security clearances on a selective basis. For example, the head of a port authority may in fact need to know what particular threats may be operating in that port. We now have the means to bring them into the loop and to do that.

As far as coordinating operations, our sector command centers are being fitted out to expand that capability. Traditionally, they have been search and rescue centers, somewhat limited in their

focus. That has been expanded, much more inclusive, much more engagement with our agency partners and private sector partners.

So that is very much in keeping with our plan for the future. We anticipate over the next several years we will see additional capabilities and the ability to share information that will be greatly expanded.

Mr. AHERN. If I might just add very briefly on the command center concept, certainly the captain outlined it perfectly. I would just add one footnote to it, that the command centers should be where they make operational sense. That is one thing as we move forward when we do evaluation of where they should be placed, it is where it makes operational sense. We continue to partner with the Coast Guard. We actually began a pilot in Long Beach that we have not taken through the entire West Coast and we are going to be adopting it for national application just for joint targeting between the Coast Guard and CBP.

I think to the question of the readiness of the ports, the president has approved through homeland security and national security presidential directives, HSPD 13 and NSPD 41, several elements that are calling for actions within the maritime domain.

The one thing that remains to be completed is the maritime incident recovery plan, which calls for the resumption of trade. Should an incident occur, how do we resume trade? I would say that the comments are in. The only thing we are waiting for at this point is that we are taking some of the lessons learned from Katrina to add that in before we presented it for final approval.

Mr. PENTIMONTI. I would like to simply add that as I mentioned in my testimony, we are concerned about the levels and amount of possibly conflicting legislative demands that come upon the industry. We have been frustrated in the past. But surely this command center deals with what is one of our long-living nightmares, and that is how we recover from incidents.

So the industry quite heavily supports the concept of having coordinated and focused command capability in each of the locations where in fact there may be incidents. So we support it wholeheartedly.

Mr. LUNGREN. Thank you very much.

The gentlelady's time is expired. The chair recognizes the gentlelady from Texas, Ms. Jackson-Lee.

Ms. JACKSON-LEE. I thank the chairman and the ranking member for this hearing, and to Ms. Harman for the author of the legislation that I am pleased to be an original cosponsor of.

Coming from Texas, we have one of the largest ports in Houston. Of course, it falls in a number of our districts. We spend a lot of time there. In fact, I spent some time there doing the Dubai port debate to assess the status of security at our port.

Let me also before going into my questioning, what I do all the time when I see the Coast Guard is to again thank you so very much for your enormous leadership during the gulf coast disaster, Hurricane Katrina. I think it is appropriate whenever we are able to applaud the enormous act of saving lives, that we do so on the public record, and I do so at this time.

Mr. Chairman and Ranking Member, I believe that this is appropriately a timely hearing, and I will take just a moment to express

a sense of consternation, when we began to debate the question on the Dubai ports issue, to find out the predominance of foreign ownership of all of our ports in America. I think if you did a statistical analysis, you would find that 70 percent to 80 percent of our ports, terminals, et cetera, are foreign-operated or owned or leased, which raises a great sense of consternation from me.

So as we proceed with the question of security and this particular legislation that focuses on container security and a number of other I think important elements. One is the strategic plan that is asking what is in place for maritime security, container security. I think we have the backdrop of questioning, why did America get to the point where we are in a sense foreign-owned at our ports? Now, the answer will be that port ownership or port operation is a global entity, and that you will find that occurring around the world.

That may be well the case, but I still raise the question of why, if it is around the world, let's just break even. Let's not be losers. Let's just make it 50/50, minimally, which is 50 percent domestic-owned, if you will, and where are the incentives for such. And Mr. Chairman, I would argue that part of the work of this committee is to look at the question of incentives and why we are in this particular predicament.

But as I raise that concern and sense of frustration and dislike, frankly, for that present posture, I also believe that we need to be proactive. I will be offering legislation that I am reviewing on a moratorium of further foreign leasing and/or ownership in America's ports.

Secondarily, I hope to offer an amendment as we move to full committee, or move to marking up this particular legislation, that deals with the seeking of existing security plans, not what will be, but what exists in the nation's top ports, so that we can begin to have a further roadmap.

It is somewhat we asked for after 9/11, which is to establish the vulnerability around America, a threat assessment plan, and I know that we might be still waiting on that at this point, some 5 or 6 years later. I hope we don't have to wait that long to find out what is going on in the nation's ports.

Let me then raise my question, Captain, to you, to find out about this seeming flaw in our system. When we began to debate the Dubai Ports World, we now have come to understand that as a terminal operator, because there was some debate saying that, oh, don't worry about it; security is not in their hands. But as a terminal operator, my understanding is that the Dubai Ports World or any other foreign operator would be responsible for the security of their terminals, and that the Coast Guard simply checks compliance with security plans.

Is this true? And how often does the Coast Guard visit terminal facilities to check compliance with security requirements? And does the Coast Guard conduct unannounced visits in order to be proactive?

Let me raise this question with the assistant secretary on this issue of ferry security. One of the glaring anecdotal stories that we can tell is that a tanker, not a ferry per se, but a tanker loaded

with weapons of mass destruction could be maybe even more destructive than the horrific act of 9/11.

My question is, what are you aware of, working with the Coast Guard, steps are being taken to secure large ferry systems? And what technology is deployed to screen cars and trucks, but not halt the system? And we know that cars or trucks would be loaded with weapons of mass destruction, get on a ferry, and enter into the water system or a port, and warrant enormous destruction.

So if you would answer those questions, and I would appreciate the comment on the idea of taking an assessment of nation's security plans in the top 10 of our nation's ports, and the whole idea, though this is a policy question, of how we can provide incentives for domestic ownership.

Captain, why don't you start out on this question of how do you check the security plans of terminal operators.

Captain SALERNO. Yes, Congresswoman.

From the Coast Guard's perspective, the ownership of the facility is somewhat irrelevant to the requirements of that facility to develop and submit a plan to the Coast Guard for approval. There are certain elements that must be contained in that plan, such as how the facility will control access, how they will guard against tampering, what areas of the facility are secure and so forth.

Ms. JACKSON-LEE. But they, the foreign entity, presents you the plan. Is that what I understand?

Captain SALERNO. The owner of the facility does, yes.

We verify. First of all, we approve that plan. If it meets all of the requirements of the law, then we do an on-site visit to verify that all of the procedures and equipment that they have stipulated in their plan are in fact in place and operational.

We routinely would visit these facilities from a formal follow-up standpoint, at least annually. However, to get to your question, how frequently do we visit them unannounced, that will vary, but it is fairly routine for Coast Guard people either from a shore-side perspective or on the water-side in a boat would visit that facility several times during the year. It may be increased depending on threat levels, what we call maritime security conditions. Most of the time these visits would be unannounced. We would verify that the people are in fact following the provisions of their plan.

Did I hit all the points that you were concerned about?

Ms. JACKSON-LEE. The salient point is that they present you the plan. They are the owner regardless of whether they are a foreign owner or domestic.

Captain SALERNO. That is correct.

Ms. JACKSON-LEE. I thank you very much, Mr. Secretary.

Thank you very much, Captain.

Mr. Secretary?

Mr. AHERN. Thank you for the field promotion, but it is the assistant commissioner of customs and border protection.

Ms. JACKSON-LEE. Oh, I like "secretary," so continue on.

Mr. AHERN. It had a very nice ring to it, but I am a career individual, so keep that in perspective.

[Laughter.]

Ms. JACKSON-LEE. Thank you, Mr. Commissioner.

Mr. AHERN. Thank you.

I think first off, on the Dubai Port World transaction, I think it is important because I have had the opportunity in eight or nine open and closed hearings in the last couple of weeks, and had the opportunity to speak before many of you over the last couple of weeks as well, but continue to put into perspective the fact of what we were talking about in that transactions.

There were foreign terminals currently operating in the United States that were going to be purchased by another foreign entity, and that cargo and containers and vessels were going to continue to come from countries of risk and they will continue to come today.

I think that is why we need to continue to focus on the act that you are talking about here today to make sure that we have a good layer of defenses in place for all modes of travel coming in from outside of our borders, but make sure that we focus on that maritime security model by having interrelated elements of the strategy beginning overseas. Those are key points for us.

Ms. JACKSON-LEE. So you wouldn't have a problem with us assessing the, if you will, status of security in the nation's top 10 ports?

Mr. AHERN. I would see no problem at all with that. I think that is a continuous process we need to be focused on.

As your question then related to ferry operations, I would first begin by stating that one of the most successful apprehensions this country has seen for an actual terrorist coming into this country to do harm was on a ferry, coming in at Port Angeles. U.S. Customs at the time actually apprehended Ahmed Ressam, and he was actually to be the millennium bomber at Los Angeles airport, and he was successfully apprehended by our officers there in Port Angeles.

We need to continue to deal with some of the same layers that we have for people coming into this country. We need to be getting the electronic manifests for ferries and cars coming on those vessels before they arrive in the United States.

I think one of the additional things that is at this point in time in its final development inside of our organization and within the Department of Homeland Security is developing the requirements for the Western Hemisphere Travel Initiative, to make sure that we have the appropriate documentation for people coning in, and ferries principally come to this country from Canada.

So we need to make sure that we have the appropriate documentation with the appropriate security features issued to individuals that we then can electronically read and transmit in advance of their arrival so that we have some predictability of who is on those vessels. Those are the key points I wanted to raise on that aspect.

Ms. JACKSON-LEE. Thank you, Mr. Chairman. I know my time is up.

I simply, if the chairman would indulge me to speak to the chairman, is to simply say this hearing is timely. I think we are at a pinnacle crisis level and I think that quick action is warranted on securing the nation's ports.

I yield back.

Mr. LUNGREN. I thank the gentlelady for her comments.

We have time to go to a second round.

I will start that off by asking Mr. Pentimonti, your organization is a foreign-owned organization, right? Your company is not an American company.

Mr. PENTIMONTI. We operate as Maersk. Maersk, Inc. is an American-based company, but it is owned by A.P. Moller, which is a Danish-based company.

Mr. LUNGREN. And you have terminal operations in Long Beach-L.A.?

Mr. PENTIMONTI. That is correct, in Los Angeles.

Mr. LUNGREN. Los Angeles. In your statement, you stated that your company has contributed to significant infrastructure investments. There is always talk about the millions, the billions that are necessary for port security. I think oftentimes we assume that that means the government pays for all of that.

What has your company done with respect to your own funds dedicated to port security in any American port, your facilities at any American port?

Mr. PENTIMONTI. With very small exceptions, our company has funded virtually 100 percent of the costs that it has incurred in putting the security requirements of ISPFSC and all of the other CBP requirements on our cargo movements incur. So we have received I think some small grants from the government on various facility improvements, but they are a small percentage of the total facility improvements that we have made.

Mr. LUNGREN. Would you have any estimate on how much your company has spent on port security improvements in your American port facilities since 9/11?

Mr. PENTIMONTI. I don't have a current number, but I could surely provide you that. It clearly is significant. We operate a number of ports throughout the East, Gulf and West Coasts, so there have been significant costs in improving our facilities to meet the requirements. In many cases, we exceed requirement levels that both the law and the regulations impose.

Mr. LUNGREN. Thank you.

Let me address this to the other three members of the panel. Yesterday or the day before, I had an opportunity to speak with some members of the longshoremen's union. One of the things they were saying is from a birds eye view from the ground, while the security efforts that we talk about here in Washington are good, they suggested that what they have seen at some of the ports they worked at is lack of coordination. That is, one company's facility security that may be fine, but there is no coordination among the company facilities themselves.

So I guess I would ask Mr. Cunningham first, how does that measure up to your observation and what you attempted to do in Los Angeles? And then I would like to hear from both Captain Salerno and Mr. Ahern.

Mr. CUNNINGHAM. I would suggest that that is probably an accurate assessment. Each of the operators do operate independent security systems. The Coast Guard, under the Maritime Transportation Security Act, each of the facilities have a facility security officer and there quarterly and sometimes more often meetings since that act was put in place.

An effort has been made to coordinate the operations and the intelligence that is gathered from the cameras and the access data through the area of the Maritime Security Committee. Grants that are being applied for by the private sector, there is a requirement now that the port authority review those grants and assure that there is some coordination.

From a perspective from the field, on the street, I would say that there is probably a dramatic need to improve and coordinate the private sector terminal security operations between themselves as well as that with the port authority and the Coast Guard.

I may add that it is very important, and here's where the federal government can play a major role, there are companies such as Maersk that are at the top of the line in the way of security. They are the Nordstrom's in security. Yet, there are others that would cut corners and will not spend the dime for security. They take the profit and spend it in other places.

So it is very important that the federal government does enact some standards to keep the playing field level, and not give one company any competitive advantage, and that is major issue in the level of security on who spends the money and who does not spend the money.

Mr. LUNGREN. Let me just follow up with Captain Salerno, then, because the Coast Guard is responsible for reviewing the security programs and so forth.

You have heard what Mr. Cunningham said about one may be doing a good job and not another. The reason this has come to my attention is that the longshoremen talked about an incident in Oakland where some fellow named Matthew Gaines, a 25-year-old individual, didn't belong at that port, and managed to gain entry at various terminals, not just a single terminal, on different occasions, and so successful was he that he stowed away on ships traveling from Oakland to Los Angeles, Oakland to Japan, and I forget where the other one is.

Now, after he had done that three times, I understand the captain of the port sent out a notice saying, don't let this guy do it again, which I am glad they did, but isn't that a suggestion that at least at Oakland we had a real problem, if one person could three times gain access not only to the ports, but also to stow away on these ships and take off?

Captain SALERNO. Yes, sir, it is a problem. That is clearly not a situation that we want to see. It is the very thing we are trying to prevent. When those types of things happen, they are certainly investigated at the local level and also receive a great deal of scrutiny up our chain of command, as was the case for this individual.

There are differences between facilities. The regulations themselves are performance-based. In other words, they set a standard that you are designed to achieve, you know, control access to your facility, for example, but it doesn't specify the methodology that you use to accomplish that.

As Mr. Cunningham mentioned, the Area Maritime Security Committee is really the focal point where a lot of coordination takes place at the port level. That is where information is shared, best practices are communicated between similar types of facilities.

A lot occurs there where people can learn from each other. It is not inconceivable that you may have different ways of doing things. There are different risks at different types of terminals. A container terminal, for example, may have a different level of security and different methodologies that you may find a bulk grain terminal, for example, even within the same port.

So there are going to be some legitimate differences, but the Area Maritime Security Committee is sort of that normalizing influence where those practices are shared. I won't tell you it is a perfect system yet. There are always better ways to do things and improvements to be made, and there are some gaps in our system, as you pointed out.

Mr. LUNGREN. My time has more than expired.

The gentlelady from California, Ms. Sanchez, is recognized.

Ms. SANCHEZ. Thank you, Mr. Chairman.

I just want to let Mr. Pentimonti know that I have a re-routing bill that you should take a look at and industry should support about what we do to resume trade if something goes wrong at one of our terminals or ports.

I am going to go back to something that Chief Cunningham said earlier, two really great points: Who is working on our ports? And what is in the box? Obviously, who is working in the ports, I talked a little bit about the trucks and how that I think is a really big gap.

After I ask a couple of questions, I hope that Chief Cunningham, you will sort of talk to some of these things because I think you have a real overall view of what is going on out at these ports, at least what we see in our own backyard.

So the trucks, and the other issue, of course, is the ID card. Who is in our ports? Who is around there?

I think another issue, too, is quite frankly with respect to the operators of these terminals. The ILWU or the longshoremen tell me that training is required. By Coast Guard regulation, training is required by the operators about what some of these guys are doing at particular points by the operators. They tell me there are plenty of operators who don't provide that training. What ends up happening is that the union has to spend its dollars to make sure that its longshoremen are doing things correctly.

And then go into what is in the box. You know, a container starts somewhere else, and we have been pushing this out to try to figure out what is in that container, and that is what the container security initiative is. I don't think it works very well. I have had that discussion with Mr. Ahern before. And then it travels here, and one of the downfalls or the bad pieces of this is, as you already indicated earlier in your testimony, is that we don't have a good system of knowing that that container didn't go somewhere else, didn't get stopped, didn't get changed, didn't get opened up, didn't get something introduced into it, didn't get switched out for some other container, before it reaches our ports.

Part of that is the whole issue of when the container gets to the port, checking the seals. And I have a feeling that a lot of operators aren't really checking the seals the way the Coast Guard regulations say they should be checked. I know that because my longshoremen tell me that. We are using cameras. Cameras can't really

tell whether a seal has been broken, whether it has been tampered with. I think we need to think about how we get back to the real basics of what is required and how we are doing that.

Or the inspection of empty containers when they come into our ports, also aren't being checked now by a longshoreman. People say, well the operators say, well we are weighing them. Well, you know, compared to what that weighs, I mean, you could put in a little suitcase of something that could be a bomb, radioactive, it could be something, who knows.

So I think it is very important that we all work together and we get these issues on the table. These are other pieces that we might be able to introduce or introduce into a separate bill.

I also want to get back to the whole issue of this, so you have this container, it leaves, it is not really tracked, it is not really sealed necessarily correctly all the way, it gets to the ports, and then we really don't check it, we X-ray it, and maybe once in a while we open it. We are completely relying on what people are telling us are in there, and many times that is not what is really happening.

More importantly, C–TPAT, we are relying on companies that we haven't even gone out to check to see if in fact they have the security things in place that you said they had. Mr. Ahern, you talked about the 2,262 validations that are in progress. And yet these companies are still receiving a reduction of their risk targeting scores. But it is my understanding that the targeting scores of these companies are already below the threshold for inspections.

So this cargo from these non-validated companies, are they inspected?

Mr. AHERN. It is a whole series of questions here. I am not sure if you would like to begin with Mr. Cunningham.

Ms. SANCHEZ. I think Mr. Cunningham, I would like to hear him address some of these issues because he has seen so much of this going back and forth in all the years he has been at the port.

What about third-party validators? I mean, you have 80 people that can't possibly check these 10,000 companies. What about having somebody else check them? Check, go out, and make the initial check on these plans that you are currently bringing in and stamping as approved and giving risk reduction for?

Mr. AHERN. I think, given the questions, I think it is probably best to start with me and maybe Mr. Cunningham would wrap it up for you, if that is all right.

Ms. SANCHEZ. Yes, I think I said let's start with you, and let's have the chief talk about what is in the box, what we need to worry about. I get the number three, the number three about let's coordinate all this. I think, you know, the model is in L.A.

Mr. AHERN. Third-party validators. We have currently, to this point, we have not actually made the determination that third-party validators would be acceptable. We feel as though this is a government responsibility, even though there is no one more disappointed in our current performance than I am, even though you have certainly repeatedly stated your displeasure with us and how we are doing at our validations, there is no one that is more concerned about getting it done quicker than I am.

Ms. SANCHEZ. I am not against the individuals who are doing this. I am just saying it is not getting done because the resources aren't there.

Mr. AHERN. And to the point of making sure that we bring enough resources to bear, we have been looking at a couple of different things. Certainly, as I stated earlier, we have 40 additional individuals that will be coming on within the next 30 to 45 days and that will get us above the 88 that we currently have on board. We have to this point resisted the notion of third-party validators. We think it is, again, a responsibility that we should be doing in the government, and not necessarily contracting it out.

However, given the current situation and the expansion of C–TPAT, which has been a good thing, we want to have more parties involved with a trusted program. We want to have the largest corporations in the industry, the importers reaching back to their suppliers, vendors, manufacturers, putting levels of security in place throughout the supply chain.

Our challenge has been getting to all those locations to do the validations, so we are reconsidering whether we should be looking at third-party validators with controls. We have now expanded over the last year since the GAO report criticized lacking having a uniform way of doing the foreign validations. We now have a very uniform scored fashion where there are weights against the findings in the overseas environment, so that we can actually provide a uniform way of doing our validations.

So perhaps we are coming to a point in time where in certain environments with certain countries that may not be of a significant risk, maybe the third-party validator has a fit for us. So we are going to be evaluating that with new eyes, but to this point we have been opposed to it.

Ms. SANCHEZ. Just to let you know, Commissioner, as you know, you can look at my record, I like federal employees. I think we have been having a discussion about TSA and whether we privatize or not, and you can certainly go back and see that I more than love federal employees.

But the scope of work, if this is to work, is so large. I just believe that if we had others take a look at those plans and validate in the structure that they are actually doing what they say they are doing. And if this auditor or validator, whoever it is, sees that there are problems, gets back to you and says, you know, you need to come out and check this company here because it is not happening.

I think there will still be more than enough work for the 88 plus 40 plus 100 plus another 100 I think by the time we look at the number of companies that would love to be in the GreenLane to get through faster.

So I would just ask you to consider that, and I don't know if anybody else has any comments other than I would like to hear from Chief Cunningham overall on who is on our ports and what do we do about the box.

Mr. CUNNINGHAM. Who is on our ports, that is a critical question that quite frankly is the very foundation of our security or lack of. The fact that when you talk about foreign operators or American operators, the issue of what, the pleasurable things, the issues that

I thought has come out of the Dubai discussions is that it has refocused security discussion on who is on our docks, and the fact that Los Angeles has foreign operators from Denmark and from Japan and Korea, and a lot of alliances that end up being both American and foreign operators.

But the truth of the matter is we still don't know whether it's American or whether it's a foreign operator who is on our docks. That is probably a fear of most Americans and a fear of the ILWU, who is on our docks. And one way of doing that, this bill I hope suggests that port identification, the TWIC, would answer that. It would answer that. We would know who is on our docks and access control would be in force right now where we are using driver's licenses and employee IDs, and that is just not acceptable. That is insufficient.

So that would answer a lot of the gaps in security that we find. The fact that empty containers are not being inspected, here again that is a cost issue with the port operator. That is an issue. It requires staffing. They are in the business to make money, and you do not make money by inspecting empty containers, and the risk assessment that has been done probably internally by their companies show that the threat, and we are concerned about the import and not the export of containers, so therefore there is very little attention paid to empty containers.

One way of handling that is mandating or providing some type of program where empties become a part of the overall security plan for the entire region. That balances the playing field so one company does not do this and the other company does not do it, and therefore you will have a gap in your security.

The issue with that customs has with the containers, what is in the box, that is so complicated. It is very, very complicated. The only solution, I believe, is just layers and layers of security that would deter the bad buys. It begins with enough will from the administration to begin the overseas examination, the inspection overseas. That is the first layer and that is probably the most important layer.

The secondary layers are those layers that take place in between, routine and unpredictable inspections by the Coast Guard in regards to vessel inspections, as well as container inspections, and then the layers that are there on the land-side at the ports. So it is a layered approach, and we are years away from having 100 percent inspection.

If Customs was to attempt to just up it 1 or 2 percent, I can imagine it would slow down our economy to the extent that we would all say why are our prices going up so high. So it is a very complicated equation that has to be balanced. But security foremost begins overseas, I believe, on the container business.

Mr. LUNGREN. Mr. Dicks from Washington is recognized for 5 minutes.

Mr. DICKS. I regret that I wasn't here for the whole hearing. I just had something I had to do. This is a very important issue.

I want to just, there was a recent article written by Steve Flynn and James Loy, former commandant of the Coast Guard. One of their major points was since the United States cannot own and control all the systems, we must work with our trade partners and

foreign companies to ensure security. A major step in that direction would be to construct a comprehensive global container inspection system that scans the contents of every single container destined for America's waterfront before it leaves a port, rather than scanning just a tiny percentage we do now.

This is not a pie-in-the-sky idea. Since January 2005, every container entering the truck gates of two of the world's busiest container terminals in Hong Kong has passed through scanning and radiation detection devices. Images of the containers' contents are then stored on computers so they can be scrutinized by American or other Custom authorities almost in real time. Custom inspectors can then issue orders not to load a container that worries them.

Now, they were talking like there are four or five companies that have about 80 percent of the containers that come to the United States. If they would impose a $20 fee like we have on aviation, that would provide the resources that the administration has filed to provide to do this job right.

I would like to get a reaction to this proposal from the panel.

Mr. AHERN. I think first from the Customs and Border Protection perspective, sir, I would tell you, and I did speak to this earlier in the hearing today, that the ICIS model that currently is in operation in the port of Hong Kong has been overstated, given its current capability. There is one lane in one of the terminals that is currently operational. There is no operational protocols or threshold settings or concept of operations that are in place. The technology is footprinted there, but it is not currently in any kind of an operational mode that has been official.

Having said that, I believe it is very important for us to take a look at the capabilities of a concept like that, putting it in an overseas environment. I think it is extremely complementary to our CSI ports where we would then have that technology.

Mr. DICKS. Yes, it fits right in with the container security initiative. Right?

Mr. AHERN. Absolutely. It is completely in line with pushing our borders out, having the opportunity to scan and screen before they are placed on a vessel for lading.

Mr. DICKS. Has the administration looked at this to see if this would be, I mean, it is under the container security, do you guys run the container security initiative?

Mr. AHERN. Yes.

Mr. DICKS. Have you looked at this concept?

Mr. AHERN. I was there in October of this past year.

Mr. DICKS. I mean, you were there, but what have you done?

Mr. AHERN. We are currently in dialogue with the commercial vendor that provides the technology package. We have actually got 21,000 data files that have been collected from the computer that actually ran the containers, again with no response protocols to take a look at what that actually might mean for nuisance alarms or regular recurring alarms, given some of the commodities or even background threshold radiation that would alarm us. Those need to be resolved before they are placed onboard a vessel for the United States.

The other thing we need to be reminded of also as far as the capabilities in the private sectors is when I met with them over

there, they are very interested in investing in this and making the capital investment to put that there.

Mr. DICKS. Hutchison is one of the leading companies in this, and they have said that they are going to do their Hong Kong-style inspection system in place within its 42 ports.

Mr. AHERN. They are certainly one of the leaders on this front and they were there when I was there at the same time in October.

The other point I think that is very important to realize here, too, is the private sector can certainly invest and deploy this there.

Mr. DICKS. They have no choice because the administration has refused to put the money up that the Coast Guard needs to do the job.

Mr. AHERN. They could certainly invest and put it there anywhere throughout the world that they like. However, one of the things that needs to be worked through as far as who is going to respond to the alarms, and there will be alarms that will come in every single day and every hour of every day that will alarm, that are nuisance or false positive alarms that need to be resolved by some government authority.

The United States government does not have authority in a sovereign nation. When we have gone out and negotiated our declaration of principles, we have to go and work through the host country counterparts. They would have to take on the responsibility.

Mr. DICKS. Couldn't Hutchison in this case go out and inspect the container?

Mr. AHERN. I don't think that that has been thought through at this point in time, and I am not sure certainly that?

Mr. DICKS. How many more years is it going to take us to think through these kind of issues?

Mr. AHERN. I think it is not quite as simple as you might like. We certainly are moving very aggressively. We are engaged with the private sector. We are looking at the data so we can make?

Mr. DICKS. Eighty-eight inspectors to monitor the compliance of the 5,800 importers who have vowed to secure their goods as they travel from factories to ship terminals doesn't look to me like an overwhelming response; 88 inspectors. That is appalling.

Mr. AHERN. That is for the C–TPAT program.

Mr. DICKS. Yes.

Mr. AHERN. That is not for CSI.

Mr. DICKS. And the Coast Guard has got 20. How many people do we have in the container security initiative?

Mr. AHERN. Approaching 200.

Mr. DICKS. Worldwide?

Mr. AHERN. At the 43 ports.

Mr. DICKS. That is not very many either, if you are serious about trying to do something about it.

Now, Captain Salerno, let me ask you another question. Does anybody else want to comment on this one first?

Mr. PENTIMONTI. Just a quick comment. The industry, you mentioned the four carriers, we are excited about the concept of figuring out better what is inside our boxes. There is no doubt. We, as Mr. Ahern has indicated, we are interested in investing. Obviously, the complexity of doing this in a foreign location and getting

response from CBP on these signals is probably the most concerning issue.

Obviously, we can, with the technology, take the pictures of what is inside the box, but for it really to improve security immediately, we would have to have a response so that we would know whether a further physical inspection were needed or in fact the box was allowed to be loaded safely on a ship, recognizing that what those pictures showed was what they should have showed.

It is that evaluation that I think, as I testified, needs some resources and needs some attention that CBP has not provided, that I believe funding is direly needed to take it forward.

Mr. DICKS. So it is the inspection part, it is once you have decided there may be an issue, then where are the people from our side to go in and look at it?

Mr. PENTIMONTI. The 80 percent of the volume that comes into the United States, as you suggest, from possibly four of these terminal operators globally, yes, I think the investment to do that, it would fit easily. But being able to take that data and have it usable so that we could make a determination, or a determination could be made that that container should be loaded and is safe to be loaded and should not be set aside to be inspected, that is really the critical step that needs to be developed in this system. We agree wholesomely with what Mr. Ahern has said that that development is something which needs to be done.

Mr. DICKS. I want to go back to the captain here. The administration has long underfunded port security efforts despite the Coast Guard identifying more than?

Mr. LUNGREN. Does the gentleman ask for unanimous consent for a couple of additional minutes?

Mr. DICKS. A couple of additional minutes.

Mr. LUNGREN. Without objection.

Mr. DICKS. Thank you, Mr. Chairman.

The Coast Guard identifying $5 billion in terms of American ports to comply with the Maritime Security Act. The same assessment showed that more than $2 billion would be needed to meet the additional guidelines issues by the International Maritime Organization, totaling about $7.4 billion over 10 years and about $1.4 billion for immediate needs. Although Congress has made an effort to provide funding, $125 million in 2004, $150 million in 2005, $175 million in 2006, $913 million since 9/11, the administration has requested only $46 million in targeted funding for port security.

Why is this, Captain? Why is there such a huge disparity here? And what would this money, if it was appropriated, what would it be used for? What kinds of things are you doing with this port security money? Why is this great discrepancy between what you found when you did the Maritime Transportation Security Act?

Captain SALERNO. Sir, the $7 billion for the MTSA implementation over a 10-year period was an economic estimate of the cost to industry to put into place the measures that were required.

Mr. DICKS. So it was never contemplated that the government would fund this?

Captain SALERNO. No, sir.

Mr. DICKS. Has the private sector funded it?

Captain SALERNO. That was intended to be a cost borne by the private sector.

Mr. DICKS. Have they funded it?

Captain SALERNO. Yes, sir, they have.

Mr. DICKS. The $7 billion?

Captain SALERNO. Well, the costs, this is over a 10-year period, that was projected in the rulemaking. We are not tracking the actual costs to private sector for the implementation. That was a cost estimate over that 10-year period.

Mr. DICKS. Well, it certainly hasn't registered high on the administration's list of priorities if they have only requested $46 million for this over 4 or 5 years. Isn't that correct?

Captain SALERNO. Sir, are you referring to the grant proposals?

Mr. DICKS. Yes.

Captain SALERNO. Okay.

Mr. DICKS. Funding for port security.

Captain SALERNO. The grants as designed were not intended to fully provide the costs of the implementation of these measures. They were as an assistance for special needs, but not intended to fully fund the cost of implementing MTSA.

Mr. DICKS. Okay, what kinds of things are they doing with the money?

Captain SALERNO. Well, there are a variety of measures that are in place, or that are proposed by the individual ports and individual facilities and vessel operators, depending on the vulnerabilities that they have identified and have brokered through the captain of the port and the Area Maritime Security Committee. These are sent up to a national process and they are evaluated and they compete for the amount of money that is available.

Mr. DICKS. Okay. Give us a few examples, if you could, of what they are doing with that money.

Captain SALERNO. Some facilities have put in for grants for physical barriers, fences, cameras, that sort of thing. Some have put in in the early stages for vulnerability assessments. We are pretty much past that phase now.

There is just a number of things as they go through their vulnerabilities and they try to close gaps, they can put in for it. Public service organizations, for example, police departments that have port security functions have put in for communications equipment. So there is a wide range of grant requests that have been submitted over the years.

Mr. LUNGREN. The gentleman's time has expired.

Mr. DICKS. Yes, thank you for the extra time, Mr. Chairman. I appreciate it.

Mr. LUNGREN. The gentlelady from California, Ms. Harman, is recognized.

Ms. HARMAN. Thank you, Mr. Chairman.

Congressman Dicks's questions point up the need, and I think I know the whole panel agrees, for a more comprehensive strategy for port security, more money obviously, but targeted at risky ports, and at multi-year improvements, which is something that this bill does.

I think this legislation as it will emerge from the House will include a lot of things that will help achieve the good suggestions

made by our panel and the good suggestions made by some in the audience like the ILWU. In that connection, I would like to strongly endorse something that Ranking Member Sanchez said, and that is more formal port security training and better terminal evacuation training for the ILWU. It is something that they need. They have requested it. Hopefully, the owners association at the ports of L.A. and Long Beach will respond favorably.

I want to ask just a couple of questions to follow-up on some of the comments already made. First of all, Mr. Cunningham was talking about the importance of TWIC cards. As I understand it, a regulation is long overdue out of DHS on TWIC cards. It is something I have spoken to Secretary Chertoff about. I wrote him a little friendly reminder yesterday.

So one question is, where are we with that, and do you agree about the importance of knowing who is on the ports and having a standard system to make sure they are who they say they are? That is number one.

Second question, and it was addressed I think by Mr. Ahern, but I am not sure, and that was about the resumption of trade. You said that the report there, or the plan on resumption of trade has been delayed so that it can incorporate the lessons learned from Katrina. I think all of us would like to learn the lessons from Katrina, but I hope that they will not further delay this report. Should we have a major attack tomorrow, I would want to know, I do want to know, and I am asking you, what are our plans for resumption of trade?

We had, as I mentioned earlier, a real-life example of what the costs of a labor lockout look like, and they are huge. So unless we have a plan in place soon, I predict that we will not only not learn the lessons of Katrina, but we will repeat Katrina. So please answer, this is for the two DHS witnesses, please answer my question about TWIC cards and about how much longer do we have to wait for the resumption of trade plan.

Captain SALERNO. I will address the TWIC. Certainly, in the aftermath of the Dubai Ports case, there has been renewed emphasis on coming up with a rulemaking on the TWIC. Not that it has been sitting idle. Over the past few years, there has been quite a bit done. Coast Guard participates with TSA on this. TSA has the lead, but there have been some technological obstacles. There has been a lot of discussions about what the vetting principles should be and so forth.

The work group has been working very hard, certainly in the last few months, to look at ways to accelerate this process, and the best I can tell you at this point is that we would anticipate a statement from the secretary within the next few weeks on where that stands.

Is it important? Absolutely. There is a significant vulnerability in our port security framework that the TWIC will address once it is finalized.

Mr. AHERN. I think to give a full answer, going back to the statements I made about the HSPD 13 and NSPD 41, there are several elements that are approved. The maritime domain awareness, MDA, has been approved. The global maritime intelligence integration plan has been approved. When we take a look at the MOTR, the maritime operational threat response, the agency roles and re-

sponsibilities, that has been approved and placed, and that gives us kind of the temporary fit until the maritime incident recovery plan gets done.

Certainly, as we did demonstrate at least within our component within the Department of Homeland Security, when we were able to close ports and redirect traffic, the commissioner of Customs and Border Protection has the authority to close or suspend activities and redirect it to other locations so that we can have continuity of operations, not suspend and then recover, which I think is a key thing as we go forward, is not hopefully to have to suspend and then begin recovery or resumption; that we try to keep it running for continuity of operations, and that is what we were able to maintain with moving vessels throughout the gulf to other locations, making sure that we also took a look at foreign-flag vessels under the Jones Act moving between ports to put relief efforts forward, and continue to keep trade going in this country as we were responding to the disaster of Katrina.

Ms. HARMAN. Well, I think that is an answer better than my question. Continuity of trade is much better than resumption of trade, and the TWIC program is absolutely critical. It should not just be a pilot project at a few ports. It should be a national program, and I hope you are hearing the urgency, at least that I attach to it.

Thank you, Mr. Chairman.

Mr. LUNGREN. I thank you.

I thank all the members of the panel for testifying, for giving us your valuable testimony, and all members for their questions.

The members of the committee may have some additional questions for you in writing and they would ask you to respond to those in writing. The hearing record will be held open for 10 days.

And without objection, the committee stands adjourned.

[Whereupon, at 2:16 p.m., the subcommittee was adjourned.]