H.R. 4954, THE SAFE PORT ACT

FULL HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

APRIL 4, 2006

Serial No. 109–71

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

36–697 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

CONTENTS

Page

STATEMENTS

The Honorable Peter T. King, a Representative in Congress From the State of New York, Chairman, Committee on Homeland Security 1
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, Ranking Member, Committee on Homeland Security 2
The Honorable Donna M. Christensen, a Delegate in Congress From the U.S. Virgin Islands 25
The Honorable Tom Davis, a Representative in Congress From the State of Virginia 17
The Honorable Peter A. DeFazio, a Representative in Congress From the States of California 22
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolian 34
The Honorable Jane Harman, a Representative in Congress From the State of California 18
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 36
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas 39
The Honorable Daniel E. Lungren, a Representative in Congress From the State of California 20
The Honorable Edward J. Markey, a Representative in Congress From the State of Massachusetts 29
The Honorable Bill Pascrell, Jr., a Representative in Congress From the State of New Jersey 32
The Honorable Stevan Pearce, a Representative in Congress From New Mexico 24
The Honorable Dave G. Reichert, a Representative in Congress From the State of Washington 27
The Honorable Mike Rogers, a Representative in Congress From the State of Alabama 31
The Honorable Loretta Sanchez, a Representative in Congress From the State of California 2
The Honorable Rob Simmons, a Representative in Congress From the State of Connecticut 14

WITNESSES

PANEL I

The Honorable Michael P. Jackson, Deputy Secretary, Department of Homeland Security:
Oral Statement 5
Prepared Statement 7

PANEL II

Mr. Clark Kent Ervin, Private Citizen, Former Inspector General, Department of Homeland Security:
Oral Statement 58
Prepared Statement 60

Page

Mr. Jonathan E. Gold, Vice President, Global Supply Chair Policy, Retail Industry Leaders Association:
Oral Statement 51
Prepared Statement 54
Mr. Christopher L. Koch, President and CEO, World Shipping Council:
Oral Statement 42
Prepared Statement 44
Ms. Bethann Rooney, Manager of Port Security, Port Authority of New York and New Jersey:
Oral Statement 61
Prepared Statement 63

H.R. 4954, TO IMPROVE MARITIME AND CARGO SECURITY

Tuesday, April 4, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 2:04 p.m., in Room 311, Cannon House Office Building, Hon. Peter King [chairman of the committee] presiding.

Present: Representatives King, Davis, Lungren, Simmons, Rogers, Pearce, Reichert, Dent, Brown-Waite, Sanchez, Markey, Harman, DeFazio, Jackson-Lee, Pascrell, Christensen, Etheridge, Langevin, and Thompson.

Chairman KING. [Presiding.] The Committee on Homeland Security will come to order.

The committee is meeting today to hear testimony on H.R. 4954, the Security and Accountability for Every Port Act, known as the SAFE Port Act.

My opening statement will be very brief, but I want to at the very outset commend Chairman Lungren, who I know is going to be here in just several minutes, and also Congresswoman Harman and Subcommittee Ranking Member Ms. Sanchez for the excellent job they have done in coming up with the SAFE Port Act.

It was legislation which last week passed the subcommittee by voice vote, and enjoyed broad bipartisan support. I believe it is a very significant step forward in addressing an issue which is obviously essential if we are to have true homeland security. If there was anything positive to come out of the whole Dubai Ports issue, it was an awakening of the American people as to just how important port security is.

Our committee scheduled these hearings and legislation on port security before Dubai Ports, but that certainly gave us an opportunity to take advantage of that moment, of that window of opportunity to move the legislation forward. I certainly look forward to the testimony of the witnesses today, each of whom is an expert in this field, which again is so vital.

Coming from New York, where I suffered the loss of many constituents on September 11, I have a very keen awareness of just how vital the whole issue of homeland security is, and also having the Port of New York and New Jersey right there in lower Manhattan and New Jersey again drives home to me how vital it is, and how essential it is that we do protect our ports.

All of us know how vital port activity is. We know the 9 million to 11 million containers that are shipped into our country. We

know the devastating impact that could result from either an attack on our ports or a dirty bomb going off in our ports. So this is an issue which must be addressed. I strongly believe that this legislation as it is written now is a very, very positive step. There may be some changes made as we go forward. It is my intention to have the full committee hearing today and then schedule a markup the week of April 24, probably on April 26 will be the day we actually do the marking up of the legislation. And then hopefully get it to the House floor as soon as possible after that as we can.

Also, our committee and subcommittee have been working closely with Senator Collins, Senator Murray, and Senator Lieberman in the Senate as they go forward with their legislation. In many ways, our legislation parallels theirs, or theirs parallels ours. So if we can again keep this process going and get bipartisan legislation coming out of the committee, coming out of the House, legislation which is closely synchronized with the legislation coming out of the Senate, I think we can see real progress being made this year.

As I speak, the chairman of the subcommittee which has done such yeoman work has entered the room. I want to again, while he is here, publicly commend him for the leadership he has shown, along with Ms. Harman and Ms. Sanchez.

So with that, I yield to the distinguished ranking member from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

I, too, join the chorus of platitudes for this bipartisan legislation. What I would like to do is to give the ranking member of our subcommittee my time to speak on this effort, Ms. Sanchez. She has been very interested and involved in this process. So if I may, I would yield the balance of my time to her.

Chairman KING. Surely, and she can have additional time after that if she wishes on her own.

Ms. Sanchez?

Ms. SANCHEZ. Thank you, Ranking Member Mr. Thompson. I appreciate all the help that you have given us on this bill, and also to you, Chairman King, for the way both of you have brought this up in a very bipartisan manner.

I would also like to commend Chairman Lungren for his willingness to work with me and others on this committee to achieve what I thought was a very successful subcommittee markup last week.

And of course, I want to thank the witnesses that are before us today to testify. I am hoping that we get more information so we make this bill even better as we move forward to mark it up in committee when we come back from the spring recess.

One of the biggest questions that I have today is regarding a CBP request from February 8, 2006 soliciting short-term private contractors to be hired by CBP to perform C–TPAT validations. I guess I am a little frustrated and disappointed that Assistant Commissioner Ahern didn't mention the solicitation at our March 16, 2006 subcommittee hearing on the SAFE Port Act, when I specifically asked him about CBP and whether it would consider using third party entities to validate C–TPAT member security plans. And then later I find out that you actually have an RFP out there on the market that was dated before the March 16 meeting.

All of us on this committee are committed to improving our nation's security, but if CBP and the Department of Homeland Security refuse to communicate and share basic information with us, that makes it really difficult for many of us to do our job. I would like to ask unanimous consent, Mr. Chairman, to add a copy of the February 8, 2006 CBP solicitation for contractors to work on C–TPAT validations to the record. [1]

Chairman KING. Without objection, so ordered.

Ms. SANCHEZ. And, Deputy Secretary Jackson, I am looking forward to getting some answers to several questions I have on the topic of that solicitation. In addition, I believe that it is a good opportunity to get feedback on the current bill. I am interested in the C–TPAT section of the bill, on the need for the implementation of the TWIC card, and what we can do to improve our ability to know what is in the box, what is in the container before it lands on our shores.

I hope that our discussion today will provide analysis of the current provisions of the SAFE Port Act, of which I continue to be a proud cosponsor. I also hope that this will be an opportunity for our witnesses to provide additional information as we go into full committee markup.

Thank you, and I yield back my time to Mr. Thompson, who will yield back, I guess, to the chairman.

Mr. THOMPSON. Thank you very much. I yield back, Mr. Chairman.

Chairman KING. I thank the gentlelady for her statement.

I now recognize the chairman of the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you, Mr. Chairman.

I would like to begin by commending your commitment to this issue on port security. No one can question whether or not this is something the committee would like to move on. Already we have held a hearing and a markup on the legislation at our subcommittee level. We will be meeting in markup session at the full committee level after the Easter recess. I understand that the leadership is committee to a floor date for this bill at the beginning of May.

In this Congress, the Committee on Homeland Security was very involved in passing the Border Security and Terrorism Prevention Act. We now look to pass port security legislation. So these are important times for our committee, ones in which we continue to establish our jurisdiction. But more importantly, we work to perform oversight over the Department of Homeland Security in such a manner that allows flexibility for the secretary, while still ensuring that those of us on this committee are held accountable to our constituents that we are elected to protect.

The Security and Accountability for Every Port Act, or the SAFE Port Act, has one primary aim: to push the United States's security borders out. It is my belief, shared by many, that if the terrorist threat reaches our shores, it is far too late. The SAFE Port Act, rather, works to build on the multi-layered defense that the admin-

[1] [Maintained in the committee file.]

istration has established so that we ensure security and accountability at each step in the global supply chain, from factories overseas to the United States seaports and everything in between.

I would say the legislation has three key ideas: first, enhancing security at U.S. ports by establishing a risk-free port security grant program with, and this is very important, dedicated funds from customs duties requiring the implementation of the TWIC or transportation worker identification credential, sooner rather than later, and I stress sooner. Actually, I just stress getting it done, and then furthering the deployment of radiation detection equipment.

Second, preventing threats from reaching the U.S. by authorizing through legislation and improving upon two Customs and Border Protection cornerstone security programs, the CSI, the Container Security Initiative and the Customs–Trade Partnership Against Terrorism, that is C–TPAT.

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

Again, I thank the chairman for taking up this important piece of legislation in this committee. I disagree with those who say that nothing has been done to secure our ports. Much has been done, but much, much more remains to be done. This bill is not contradictory with what the administration has done, but rather builds on the foundation it established, but we need more than a foundation. We need a super-structure of legislation which means real, live programs that have a continuing basis.

I would like to thank the ranking member of my subcommittee, Ms. Sanchez, for the work that she has done on this. I would also like to thank Congresswoman Jane Harman for co-authoring the bill with me as well. We were working on this long before the Dubai controversy erupted. The Dubai controversy allows a focus on this issue, which we may not otherwise have had. I think it assists us in moving forward with all due dispatch. I think it is a testament to the leadership and direction of the committee that partisanship has been put aside in order to create laws to protect our homeland.

I thank you, Mr. Chairman.

Chairman KING. I thank the gentleman for his statement, and again commend him for his leadership on this issue.

Let me remind members, but under our committee rules, opening statements are limited to the chair and ranking members. However, all members are entitled to submit opening remarks for the record.

With us on our first panel today is the deputy secretary for the Department of Homeland Security, the Honorable Michael Jackson. Mr. Jackson is doing a fine job, an outstanding job, and is certainly dedicated to this country. He has proven it in the past and he is demonstrating it more in his service today at the Department of Homeland Security.

Mr. Jackson, as we discussed, your full statement will be made part of the record. If you could try to keep your remarks to 5, 7,

8, minutes, it would be greatly appreciated. I can assure you that there will be many questions asked by both sides of the aisle here.

So with that, I recognize Secretary Jackson.

STATEMENT OF HON. MICHAEL P. JACKSON, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Mr. JACKSON. Thank you, Chairman King, and thank you, Ranking Member Thompson. I am very grateful to this committee for the work that they are doing and grateful for the opportunity to talk today.

Maritime security is an important and vital part of our overall homeland security work. We are confident that we have made transformational progress since 9/11, but I am very much in agreement with the members who have stated that much remains to do ahead. We need to and we will build upon the base that we have created, but there is much more work to do.

Since September 11, we have put significant resources at this. We are spending at the rate of about $2.5 billion this year on maritime security. And if the president's fiscal year 2007 budget is enacted, we will have spent some $9.6 billion in the period fiscal year 2004 to fiscal year 2007.

Today, I would like to talk particularly about the path ahead to strengthen cargo security from a risk perspective. We have focused at the department principally on weapons of mass destruction, not exclusively, but this very high-risk and very high-consequence threat merits particular focus. I am going to start by just talking about a couple of principles that we bring to this table. I think honestly they are very much embedded in the work that the committee has done and that the subcommittee has done in this area, very much in intellectual and philosophical alignment about the approach.

First, what we are looking for is a layered system supporting a global network. We are looking for multiple, mutually reinforcing tools which can prevent single-point failure, so it is actually multiple tools around this network that we have to focus on. Some layers are more immediate and obvious, like screening a container. Others like nuclear nonproliferation, help us provide a context where we can guarantee that this work is made more solid.

Security is seldom adequately delivered via a single silver bullet. It begs the obvious, but we have to note that the framework for this, it is a global system. We don't control all the moving parts. Most of this work is done in the private sector. The vast bulk of it is done in the private sector. It also involves work with multiple foreign governments.

To push security out the border has been a second principle that we have to face, and it is one that is embedded in the SAFE Port Act today that we are discussing. It strengthens our hand to partner with governments, so this is a third element that we consider crucial to our success, a series of government-to-government partnerships and also leveraging groups such as the World Customs Organization, the International Maritime Organization, and the International Standards Organization. So that is the context for it.

There are really eight moving parts to this equation. Your bill in one way or another touches these eight moving parts. First, the

components are vessel security, personnel security, port infrastructure security, and cargo security or the security of container and break-bulk moving through the system. If you take those four elements and you say we have to address them both domestically and internationally, you have eight components to focus in the work that we have ahead.

I would like to start just by beginning briefly to discuss two particular areas that I think offer high up-side potential for increasing security. First is a series of things that we collect under the idea of secure freight; and second is TWIC, the transportation worker identification card. I will just say a word about those and a word about the bill, and then I would be happy to take questions, sir.

On the first, what we have in the initiative that Secretary Chertoff has launched under the name of secure freight, really captures some of the core moving parts that you are also discussing in your legislation. First it is better targeting; and second, it is enhanced inspection tools.

Better targeting, the automated targeting system, ATS, is a first-generation tool to gather data about what is in-bound, essentially by scraping the weigh-bill electronically and by comparing this with a large historical database about container movements abroad. We augment that by conversations in the CSI program, the Container Security Initiative program, on a port-to-port conversation so that when we find a container of concern, we then can drill down with those officials and bring additional data to the table.

This is a first-generation tool. It is a good tool. It is not a perfect tool. The next generation tool we would like to suggest really requires us to re-think in a much more aggressive and innovative way what data we get, how we fuse it together, how we collect it, and how we share it internationally, and how we use it to drive the container profiling that needs to happen when we go into an assessment of each container.

I won't try to unpack that fully, but I would just say that I think that we can gather data that exists in multiple entities' databases, fuse it together in effect to create a pre-history of container movement that will allow us to understand much more clearly the risk associated with that particular move.

Second, enhanced inspection tools. Better detection systems can be deployed both at home and abroad. At home, our goal is to have 100 percent inspection of all containers as they depart U.S. ports into the country. Abroad, our goal is to increase materially the number of containers inspected by radiation detection tools and by non-intrusive inspections such as large X-ray-type of devices.

The Domestic Nuclear Detection Office, which I am very grateful to the committee for authorizing, is focused on bringing a new generation of tools here. Secretary Chertoff is just returning from a trip overseas to Asia and has inspected the integrated container inspection system, the ICIS pilot. After extensive discussion with industry, we believe that this pilot and its underlying technology and business concept offers a very valuable opportunity for us to strengthen in a significant way the data that we are gathering.

Second, I would like to talk just a little bit about the transportation worker identity card. We can talk in conversation. I am just going to tell you, Mr. Chairman, we are committee to this. Chair-

man Lungren, we are committed to this. We are sharing the same view that you have. Get it done, get it out and get it going. It has been too long in coming. I want to tell you that we are prepared to do exactly that.

On this particular legislation, we share many, many things with you in agreement. There are some tweaks and suggestions that we have. We believe that the work of the manager's substitute and particularly the work, Chairman Lungren, that you have done, and Congresswoman Sanchez, Congresswoman Harman, we are very, very grateful for the cooperation that you have brought to this. We think that there are very valuable tools here.

I have already talked about the next generation of ATS. The bill calls for increases and improvements here. We are committed to doing that. That is what secure freight is about. We are open to ideas also. The radiological threat we have talked about, and the tools that we bring to this, are part of what you are talking about. You have asked for strengthening C–TPAT and CSI. We are in agreement that we need to do so.

You have authorized the creation of an under secretary for policy office that would be focused on cargo security. We are in agreement. I will tell you that I have already interviewed people for this position and we are preparing to move right ahead with is.

Port security grants, we would ask you to consider the administration's proposal for transportation infrastructure protection programs which would bundle maritime security and transit security and a few other programs together. As we look from time to time at changes in the risk profile, we see that we would like flexibility at the local level for us to be able to put significant funds into infrastructure protection at the local level and to give discretion there. We think bundling them offers a significant opportunity.

So, Mr. Chairman, I will just stop here and say that I am very grateful for the work that the committee has done. I am eager to continue to work with you, and I look forward to passage of a bipartisan piece of legislation that will help us strengthen our work in the maritime domain.

[The statement of Mr. Jackson follows:]

PREPARED STATEMENT OF HON. MICHAEL P. JACKSON

Chairman King, Ranking Member Thompson, and members of the Committee, I am pleased to be here today to discuss maritime cargo security in general, and in particular H.R. 4954—The SAFE Port Act.

Maritime security has been important to the United States since its earliest days. Today we have an efficient maritime transportation system that acts as the backbone of the global economy. That transportation system can also be used to move dangerous cargo to our ports and cities. Any disruptions to that system will have immediate and lasting consequences for our economy and the world at large. The Department of Homeland Security (DHS) commends the work of this Committee in addressing the vulnerabilities of containerized cargo. Our leadership is grateful to this Committee for this hearing and your work to pass important legislation to strengthen maritime cargo security.

Since September 11, 2001 we have made transformational improvements in the extent and quality of the layered system of systems now deployed to strengthen cargo security. This year, the DHS will spend $2.5 billion on maritime security. Overall, the Federal Government is spending $2.8 billion, including the Department of Energy's Megaports program. If the President's FY 07 budget is enacted, we will have spent some $9.6 billion in this area in four years (FY04–FY07).

Today I would like to talk particularly about the path ahead to strengthen maritime cargo security from a risk perspective. We have focused specifically on the

Weapons of Mass Destruction (WMD) threat because of its potential impacts, but I will also touch on measures that will strengthen our ability to detect all forms of contraband.

A Layered System of Systems Supporting a Global Network. First, a brief word about our overall approach to maritime cargo security. Our security doctrine is grounded on a commitment to deploy a strong, layered system of security systems. By deploying multiple, mutually reinforcing security layers and tools, we diminish the risk associated with failure at a single point. Some layers may have a more immediate and obvious security function, such as the physical inspection of a container by Customs and Border Protection (CBP) field agents. Others, such as the Administration's work in global nuclear non-proliferation are complementary, aimed at making it more difficult to acquire WMD components. Security is seldom adequately delivered via a single silver bullet.

It begs the obvious, but bears noting, that we are talking about a *global supply chain* that serves an *interdependent global economy*. Thus, a second doctrinal component of our cargo security strategy has been, where possible, to push security measures out beyond our borders. Close partnerships with the private sector are essential because the private sector owns most of the assets and moves the goods. CBP's Customs-Trade Partnership Against Terrorism (C–TPAT) is an example of such a partnership program.

It strengthens our hand to partner closely with other governments, which is why bilateral and multilateral solutions to supply chain security continue to be a focus for this Administration. The Container Security Initiative (CSI) and our work with the World Customs Organization, the International Maritime Organization and the International Standards Organization have improved security.

Existing Security Architecture. The existing security architecture consists of four core components: (1) vessel security; (2) personnel security; (3) cargo security; and (4) port facility security. Some elements of each of these four components are focused abroad, others at home—thus there are essentially eight areas of activity that capture most of the programmatic focus of our supply chain security work. The draft legislation that is the focus of this hearing appropriately seeks to strengthen most of these categories.

I would like to discuss two particular areas that present significant near-term upside for improving security: (1) improvements regarding DHS's targeting of highest-risk containers and our tools used to inspect containers; and (2) deployment of the Transportation Worker Identification Card for unescorted access to U. S. ports.

Secure Freight. The Department's Secure Freight initiative has two major components: better targeting and enhanced inspection tools.

Better Targeting. CBP's Automated Targeting System (ATS), which is used by the National Targeting Center and field targeting units in the United States and overseas, profiles inbound cargo and identifies high-risk cargo 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 therefore should be scrutinized overseas or at the port of entry.

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 container scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

ATS is an extraordinarily powerful "first generation" tool, and a more sophisticated, next-generation tool is under development at DHS as part of the Secure Freight initiative. ATS data is derived from filings of cargo waybills and an extensive historical risk scoring algorithm derived from years of data about containers and inspections.

The next-generation tool will fuse existing data along the supply chain gathered from multiple actors who touch the box from the order, to container origin, to destination. This data aggregation would, in my view, best be fused by a third party intermediary—perhaps formed by the industry itself. The U.S. government would then receive this richer set of data about each container move in advance of lading overseas. It would then inform CBP's container risk assessments. Ideally, the U.S. government would certify one or more such qualified entities formed for this purpose, and would set standards for such data fusion. The intermediary would be rigorously audited.

This approach is the natural extension of the requirement to have better data upon which to score risk of inbound containers. It would support not only the needs of the United States better to understand and assess risk of inbound containers, but also could serve the exact same needs for other nations. This would serve to improve

security in the global cargo network and in more nations. This next-generation tool will not grow overnight. But stronger container profiling is possible, and I am convinced that we can make great progress in the near term. I ask this Committee to support our efforts in this area, and would welcome an opportunity to elaborate further in response to your questions.

Enhanced Inspection Tools. Better detection systems can be deployed both abroad and at home. At home, our goal is to have 100 percent inspection of all containers as they depart a U.S. port headed into our country. Abroad, our goal is to increase materially the number of containers inspected by radiation detection tools and by non-intrusive inspections, including large-scale X-ray devices. The Domestic Nuclear Detection Office (DNDO) recently tested new and better fixed, mobile and handheld radiation detection equipment that can be deployed to ports of departure, ports of entry and the marine environment.

In this regard, I would note that last week Secretary Chertoff was in Hong Kong and saw first-hand the Integrated Container Inspection System (ICIS) pilot program underway there. CBP is engaged in a technical exchange to evaluate how the data gathered by ICIS can be used to strengthen our inspection capabilities. After extensive discussion with industry about the ICIS pilot and its underlying technology and business concepts, I am highly optimistic that this pilot can point the way to a collaborative network that can significantly enhance CBP's capabilities physically to inspect a larger number of containers from points worldwide. I'd be happy to discuss with the Committee DHS's thought about how this might develop.

Transportation Worker Identity Card (TWIC). On Friday of last week, the Transportation Security Administration (TSA) published a "request for qualifications" seeking firms who are appropriately experienced and interested to help DHS deploy certain components of the TWIC program. The TWIC architecture, compliant with FIPS–201 technical architecture, will provide an open standard and ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector. This is the first step toward operational deployment of the TWIC program for unescorted access to all U.S. ports. This day has been too long in coming.

This deployment includes accelerated and parallel rulemakings by both TSA and Coast Guard. And it includes a procurement needed to help launch the operational program. Secretary Chertoff has given his team instructions to get this done as quickly as possible. Further details will be forthcoming as part of the rulemaking and procurement actions. This tool will add another valuable layer of security to domestic port operations and will strengthen overall supply chain security.

H.R. 4954—The SAFE Port Act. The Department is committed to moving forward on all eight areas of activity regarding cargo security. We believe that there is much in this proposed legislation that will provide the springboard for further advances. We would like to commend the Manager's Substitute Amendment that the subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity passed last week, which we believe provided further improvements to the legislation. At this point I would like to offer comments on a few specific sections of the SAFE Port Act.

Next Generation ATS. Your legislation calls for improvements in CBP's ATS capability. As my previous discussion of the Department's Secure Freight Initiative shows, we agree that this already powerful tool should be made stronger. We very much look forward to working with Congress on operational details of a second-generation system.

The Movement of Radiological Material. The capacity to detect and identify the illicit movement of radioactive materials across our borders in the commercial supply chain is a critical concern of the Administration. DNDO is working closely with CBP to develop a new deployment strategy that will provide an optimized mix of current and next-generation systems to balance capability, coverage and cost. That deployment strategy will result in screening 98 percent of all containerized cargo crossing the southern border by fiscal year 2006 and at seaports by fiscal year 2007.

Domestic Nuclear Detection Office. DHS appreciations the authorizing language for DNDO included in your legislation. The legislation establishes DNDO to detect nuclear and radiological material, improve that detection capability over time and develop a global detection architecture to ensure linkages across Federal, State and local agencies. We appreciate the Committee's recognition of the important work of DNDO by including this provision and formalizing the role of DNDO in protecting our nation against this threat.

Improvements to the Customs-Trade Partnership Against Terrorism Program. The DHS supports any effort that aids the Secretary in strengthening and improving the overall security of the international supply chain and U.S. border security. The DHS considers the C–TPAT section as particularly constructive because it does not seek

to establish regulatory requirements for a voluntary government and industry partnership program, yet it supports strengthening C–TPAT. Additionally, the provision on the utilization of third party entities to conduct validations is a concept that merits near-term serious exploration.

Director of Cargo Security Policy. The legislation calls for the establishment of a Director of Cargo Security Policy to coordinate Department-wide cargo security policies and programs with other executive agencies relating to cargo security. We strongly agree with such a proposal and greatly appreciate both the Committee's support for the creation of an Under Secretary of Policy as called for in the Department's 2SR recommendation and this modification to our organizational findings. We are moving ahead to implement this recommendation by actively recruiting a well-qualified individual to lead this effort.

Port Security Grants. While the legislation does not specify whether the port security grant program authorized is part of the Administration's proposed Targeted Infrastructure Protection Program (TIPP), I would like to take this opportunity to reiterate that the Administration supports the creation of the TIPP to enable increased funding for protecting infrastructure on the basis of risk that may, if warranted, increase funding for ports. Under the President's FY07 budget request, $600 million is requested for the TIPP grants, which would allow additional resources to flow to port security needs based upon the most up-to-date threat risk assessment.

Technology Investments. The DHS fully supports the concept of investing in research and development to improve our maritime cargo security. The DHS is engaged in a substantial amount of research and development on maritime cargo security solutions, which includes bringing to bear the innovation and market forces of the private sector. While we differ in our method and timing on container standards, we agree in the need to launch a six-sided container intrusion detection system. The DHS is participating in a number of development efforts regarding container standards. We must ensure that any standards are based on the right technology, lest the rush to endorse a standard could result in operational practices that do not appreciably enhance security and may unintentionally impede international trade.

Conclusion. The Department is working closely with other government departments and agencies, with industry, and the international community to establish workable solutions to improve supply chain security. We recognize the challenges that face our programs and the importance of protecting our nation from terrorist threats to our vital economic engine. We are making significant progress. I would like to thank the House Committee on Homeland Security again for this opportunity to discuss our efforts and comment on this legislation which is so important to the Department and the nation.

This completes my prepared statement. I would be happy to answer to any questions you may have.

Chairman KING. Thank you, Secretary Jackson, for your testimony.

I have two basic questions at the start. On the issue of container security, specifically dealing with CSI, the container security initiative, a number of critics, including Mr. Ervin who will be testifying later today, raise the point that less than one-fifth of the containers that we believe should be inspected abroad, I think about 17 percent, are in fact inspected. We have heard that in France, they refused to inspect about 60 percent of the cargo that we deemed to be high risk.

Considering that, how secure should we feel about it? Again, these is just the cargo that we ask to be inspected. If 60 percent of that is not inspected, it seems to me that we are leaving ourselves very much as risk. What do you see is the way to improve that? What are the prospects for improving it?

The second question then you can answer is on the TWIC. I know you said that they are going to be done, but I would ask if you could tell us why there has been such a delay up until now. I know you want it done as quickly as possible, you say, but what does that mean? Are we talking about next month or 6 months from now or 1 year from now? Because this to me, and especially as there are several ongoing investigations around the country

which indicate that are very serious issues with people working at the ports who should not be working there. Each day that goes by, I just think increases that risk.

Secretary Jackson?

Mr. JACKSON. Let me say just a quick word about the CSI examinations. There has been some misunderstanding about the metrics, and I would like to make a distinction to help further unpack this particular question you are asking about. What portion of the containers that we ask to be inspected by a foreign government actually are inspected? The distinction I would like to make is a distinction between referral and request. When we do the initial targeting and begin our profiling of a container before it is loaded onto a ship, we have many, many, many cases where we ask the foreign government if they have additional information about what we consider to be a preliminary container of concern.

That is what the CBP would refer to as a referral. So we make a referral, and we say, can you give us more information about this? For example, we may have scored higher for risk a container that is being moved by a firm that we have little knowledge of, but it may be that the port and the customs service in the foreign government has extensive experience with that particular firm. They may export to multiple other locations.

So we can use these referrals to gather additional data. We do that routinely. And then for those that we want to make a specific request, we do that and ask for a request that those containers be opened or inspected through physical means. Our numbers for these examinations reached towards the 89 percent range when we actually make a request that they open the container or further examine the container in a physical way. So that number is on aggregate higher.

There are some ports where we honestly have to work on that relationship to keep it strong and to make that connection work. Some of these containers are loaded onto ships and come our way. If we have flagged it, 100 percent of those containers are inspected through physical means when they arrive on the shore. So we agree that the idea of pushing the borders out should get the maximum number of containers inspected with tools and cooperation overseas, and that is where our focus is. In cases where we need to put extra push on our partners overseas, we are thoroughly committed to doing that and helping them understand the importance of this.

Chairman KING. We are very interested in the comments of the second panel when they come on. That is an issue that we have to address, I think, and I appreciate your testimony.

Now, on TWIC?

Mr. JACKSON. Yes, sir. I would say it probably will come up later when we talk about radiation, this idea of trying to get better radiation inspection overseas is something we are also very strongly committed to and would like to discuss with the committee as well.

On the question of the TWIC, Mr. Chairman, I can't tell you why it has taken so long. I can tell you I am very impatient. I can tell you Secretary Chertoff is very impatient. And I can tell you that our entire team is focused on this as a very high priority issue. I am loathe to give you an exact date, but it will be measured in

terms of months, and not years, when we are actually beginning to issue these cards.

We have put out as of last Friday a request for qualifications for what is one of three moving parts to make this work. One moving part is to get some outside consulting firms and outside vendors who would be willing to prepare to do on validation by us and with certification from us and by auditing from us and with oversight from us, some of the intake process that we would need here to gather fingerprints and data for the TWIC background investigation tool.

Secondly, we are going to need two regulations: one from Coast Guard and one from TSA to make this work. We are in the accelerated drafting phase on both of those rules. We have a concept of how this will work. We are leveraging three pilots that we did earlier. We have an IG report on internal studies of how to strengthen the software platform that we will use here. We have an operations concept of how to get the cards back and forth to the frontline.

So we are moving very aggressively at this. We have been instructed by the secretary to press the margin of time for every single stage of this: NPRM, final rule, and award of contract to move forward. We are going to do that very aggressively.

Chairman KING. Thank you, Mr. Secretary.

The ranking member?

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Mr. Jackson, the Senate Homeland Security Committee report recently stated that only 17.5 percent of high-risk containers are inspected overseas. Now, what that means on the other hand, is that 82.5 percent of the high-risk containers arriving in the U.S. are not inspected at all. Moreover, the GAO in 2005 found that inadequate staffing resulted in 35 percent of containers not being targeted, so now these containers were never subject to inspection.[2]

I, along with some of the other members of this committee, have tried to increase personnel at our seaports to accomplish these things. Your budget request is $12 million for 106 seaport inspectors. Do you think this is enough?

Mr. JACKSON. Yes, sir. Let me start with a distinction, and then I will answer the budget question if I can. What we are doing to look at containers, the distinction between screening and inspection is the crucial one. We are screening through use of automated targeting and container profiling 100 percent of all containers inbound into this country. We are inspecting 100 percent, every single one of the containers that we identify as high-threat or high-risk containers. Of those, we screen them in two locations: overseas and then domestically when they arrive in our ports.

We are working on a third leg of this screening process, which is to screen 100 percent of all containers in the United States before they leave a port on their way out the door. We are going to be at 98 percent of that, of all containers, with the plan that we have on the table, by the end of next year. We are making very, very substantial progress. We are a little over 51 percent right now.

---

[2] GAO, *A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO–05–557 (Washington, D.C., April 2005).

Mr. THOMPSON. Excuse me. So you are saying to me that nothing comes to our shores without being inspected?

Mr. JACKSON. Screened. Everything is screened, meaning we do a risk assessment, and then inspected, which is using physical tools such as radiation or large-scale X-ray devices.

Mr. THOMPSON. I don't want to get caught up in semantics between screening and inspection. So if we don't have the personnel to inspect everything that is targeted and 35 percent of that is never even identified for inspection, you don't count that?

Mr. JACKSON. We do inspect 100 percent of all high-risk containers. That is to say, we use radiation portal monitors or large-scale X-ray machines or we use physically opening so-called "devanning" of the container.

Mr. THOMPSON. So is your testimony that the GAO report was wrong?

Mr. JACKSON. I am not familiar with the specific passage in the GAO report. I would be delighted to look at it, sir, and to provide written comment on the specific observation there.

Mr. THOMPSON. I am just trying to make sure, because the public and members of this committee are told time and time again that many items come to this shore not inspected, and some not screened. So now you are separating the two, that 100 percent screening occurs—

Mr. JACKSON. Yes.

Mr. THOMPSON. —before it reaches out shore. That is your testimony.

Mr. JACKSON. Yes, sir.

Mr. THOMPSON. And so therefore the need for additional personnel in the screening area, we don't have it?

Mr. JACKSON. Here is what I would say in the screening area, sir, and I am not convinced we wouldn't use additional personnel in this regard. In my written testimony, we talk about bringing the next generation of screening technology and tools to understand better and more richer the data that is associated with the pre-history of a cargo container move. There is area for growth in this to get a second-generation tool. We are proposing with the Secure Freight Initiative to begin exactly that. I think we can do a better job on that.

I am not trying to say a story that everything is happy and don't worry. There is work to improve on the screening side. On the inspection side, we can do and should do more overseas, as possible, with the investment and the tools, especially radiation detection tools, and large-scale X-ray devices. We will do more here in the domestic environment as well. So if I made those eight buckets of activity for us and said that there are four essential areas of focus, one of them overseas, that is four, and in the inland domestic environment, that is eight. The screening work takes place in the overseas environment before it comes here. The inspection work occurs both domestically and overseas.

Mr. THOMPSON. I see my time is up, Mr. Chairman. I will submit the other questions for Mr. Jackson to respond to.

Chairman KING. Fine.

The gentleman from Connecticut, Mr. Simmons?

Mr. SIMMONS. Thank you, Mr. Chairman.

I thank the witness, Mr. Jackson, for his testimony.

I also commend my colleagues for doing what I think is a really terrific bill here, working in a bipartisan fashion to come up with something that is good for America's ports and good for America's homeland security.

I would like to focus a little bit on the issue of $800 million in port security funding. We have 361 ports in America, according to staff information in my notebook, and $800 million sounds like lot of money, but if you do the math, and I already have, that is about $2,216,066.50 per port. When you consider that some of our ports like New York, Baltimore, Long Beach, California, Louisiana, are really large and very significant ports, my guess is that they are very quickly going to consume a lot of those security dollars.

So that leaves some of the smaller niche ports, if you will, largely unprotected. I have a particular interest in New London port, which is the host to a nuclear submarine base, a nuclear submarine manufacturer, the Coast Guard Academy, the Coast Guard R&D Center, both the Amtrak and the I–95 Boston–New York lines, Pfizer Global Headquarters and various other resources located in a very compact area in a port that has ferry service to New York and to Rhode Island, but does not appear on the list of ports at risk. In other words, the professional assessments that we have had before this committee on those ports and areas at risk does not include the New London port.

How can we anticipate that the Homeland Security Department is going to allocate these resources, when it seems to me that $800 million is really not an adequate amount? How can we be sure that some of our smaller ports located in less populated areas are going to get the assistance they need?

Mr. JACKSON. Yes, sir. Let me just try to unpack a couple of components of your excellent question.

On how to give some flexibility to provide port funding and port grant funding, this is an important area. This is why we have proposed the so-called TIPP program, which would allow for flexibility. If you area needs to put your infrastructure protection dollars more in, say, rail security rather than port security, it would give you flexibility to see that that happens. If it is port security that is the highest on the priority list, then it would give you flexibility to do that.

So we proposed $600 million this year in this consolidated grant program. It is a substantial increase on the order of magnitude, I believe without checking the exact numbers, of twice what aggregated dollars would be for the individual programs. So we proposed a substantial increase in this infrastructure protection grant money available for fiscal year 2007.

In the current year, we are trying to focus with the most care possible on the areas of highest risk and we are trying to identify very specifically the types of risks that we think are the highest impact and also present the greatest consequences, a Cole-type of attack, for example. So we have structured the grant guidance to say, come back with recommendations to focus on the things that matter most.

We had a very interesting experience with that last year. Some people did that very, very well, and got good money. Some people

ignored that, focused on much less risky items, and didn't get as much money. So we are trying to focus on the risk and then we are trying to say, look, let's look as we go through this year and see if we need to adjust the numbers, the size, the eligibility criteria. We are in the final stages of that for port security grants this year, and that is a topic that the secretary and I will be taking up imminently.

Mr. SIMMONS. Thank you for that response. I think this is something that we will continue to watch very closely.

Again, I thank the chairman and the ranking member for this excellent hearing today.

Chairman KING. I thank the gentleman.

The ranking member of the subcommittee, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Again, thank you, Mr. Jackson, for being before us today.

I alluded earlier to a subcommittee meeting that we had, a congressional hearing on this particular bill, on March 16. I had asked Assistant CBP Commissioner Ahern about using third parties to conduct C–TPAT validations. He replied that CBP was looking at using third parties for certain functions, but that generally he believed that this was a federal responsibility to conduct these validations. He was pretty adamant about that.

I asked how many people he had onboard to conduct those validations, and he said that he had 88, and that he had about 40 more scheduled to be trained and brought on shortly. While he said that CBP was looking at the possibility of using these third party validators, in fact his agency had already issued a solicitation to use contractors to validate the security plans of C–TPAT members. According to the solicitation, CBP will use an intermittent contractor to perform validations, training and provide technical assistance.

So knowing that, I would like you to answer the following questions about that process. First of all, when was the department planning on telling the committee that it was issuing invitations for contractors to conduct C–TPAT validations? And why didn't Mr. Ahern just simply tell me that he had solicited for this already?

Mr. JACKSON. I am at the disadvantage that I saw the document that you are referring to after I had already sat down at this table. But let me give you my understanding of it, and a pledge, Congresswoman Sanchez, that I will get you immediately the facts that you need to answer these questions fully.

What I understand is that CBP has put our periodic requests such as this one to be able to hire individuals to work on the CBP team with them. For example, with one of these recent solicitations, CBP hired 19 retired Customs Service officers to come back in and work for CBP and to help manage the process of doing validations.

I would make this distinction from that type of internal hiring, to the third party screening. Let me just say that I understand CBP has some reluctance to experiment in this area, but I would tell you that after some recent discussions, it is the determination of the secretary and the deputy secretary that we do not share that hesitation and we are eager to try to experiment along the lines that your bill proposes.

This procurement, according to what was just told to me, is not that movement. So let me validate that for you and let me get additional details about it, and help unpack for you the staffing plan and how we use people in this. I think the third party validator is a powerful idea. It is a force multiplier. It is one that if controlled properly can get us farther down the road faster. I am very much open to that.

Ms. SANCHEZ. I am concerned about the fact that you have certified over 5,000 companies, but really only validated about 1,500, and yet you are giving lower score points to these companies that really haven't proven that they have, or we haven't seen that in fact they are putting into place the plan that they have submitted to you. So if you are trying to tell me, then, that you believe that that solicitation is for prior people who worked for the agency who are now going to come back as contract employees. Is that what your belief is?

Mr. JACKSON. That is what I was told, but again I would like to get factual confirmation there, ma'am.

Ms. SANCHEZ. What about these 40 new people that Mr. Ahern was talking about? Are they going to be federal employees or are they also contract employees?

Mr. JACKSON. I would like to get the facts for you ma'am before I speculate with you about the 40.

Ms. SANCHEZ. Okay. And lastly, what protections have you put in place to ensure that C–TPAT member companies' proprietary information is protected, if you are using contractors or if you are going to use outside third party validators?

Mr. JACKSON. There is a requirement and protections in employment that people sign to preserve private data and nondisclosure agreements. These are enforceable by sanctions from us. So there are multiple tools in the hiring process to protect this data.

Your underlying question, as we grow C–TPAT and as we look at the question of third party validators, is the core question. How do you protect privacy, how do you protect business confidentiality, and how do you make sure that we can get that data in a timely way and use it? These are all core components of a successful program, the type of program that this legislation calls for.

Ms. SANCHEZ. And then that would also follow to what type of solicitation is really out on the street.

Mr. JACKSON. Yes, ma'am.

Ms. SANCHEZ. If it is just to the contractor, that is different. But if it is really for third parties, then these types of assurances should be in place.

Mr. JACKSON. Yes, ma'am. I do not believe this is a solicit third party contract. I have been told that that is not the case. I will, again, get more facts, but if we do that, we are going to do it in a very public, very deliberate way. This committee is going to know about it. We are going to ask your counsel on how we proceed. We are looking as a reference point in the legislation that you have drafted, and we will do this with all due protection, all sense of urgency, but care in the structuring of the program.

Ms. SANCHEZ. Thank you.

Thank you, Mr. Chairman.

Chairman KING. The gentleman from Virginia, Mr. Davis?

Mr. DAVIS. Thank you.

Mr. Jackson, I am very supportive of the framework that is established by this bill to further strengthen the C–TPAT program. I think that an independent third party validation process really offers great promise in ensuring secure shipping, while helping to manage costs within reasonable limits.

Now, a process which leverages private sector efficiencies and competition, but meets stringent standards set by DHS, is far preferable than government hiring thousands of new employees to conduct the work, as well as the cost allocation that comes with that in terms of who bears the cost.

A key component in such a program is that companies engaged in third party validation should be financially independent of the shippers that are evaluating and free of any other entangling business or other relationships. I am pleased to see that your statement says third party validations merit near-term serious exploration, but could you share further thoughts on this? Do you think independence is going to be critical in this?

Mr. JACKSON. Yes, sir, I do. I think that that is an important component, and make sure that we have insularity from any possible business conflict of interest that is there in that process. In the same way, the government validators have to have that same kind of assurance. So I think that any successful program in this area would require us to be very explicit and to set stringent requirements to make sure that is preserved.

Mr. DAVIS. When you note that cargo coming in is 100 percent screened, what does that mean, to "screen" it? When you go through an airport and you are screened, it means one thing, but with cargo, it means something else.

Mr. JACKSON. Yes, sir. This is the confusing world of DHS vocabulary. I apologize for it and I will try to explain it as best I can.

It is a different thing in the airport screening environment. We call that physically walking through a machine that inspects you in one way or another through X-rays or other devices. In this world, the screening, if you think of it as profiling, we are trying to profile a container based upon the data that we have about that container, and score it for risk. In doing this, we gather today information from the weigh bill, I believe it is some 22 variables, I may be wrong on the exact number, but on that order of magnitude.

What we do is use that to score risk. We look at who is shipping it, who are they shipping it to, who has touched it, what do we know about what is said in here, what do we know about the various different variables that go into assessing risk. Then, and attached to that is a very significant database of historical records of individual shippers, of pattern analysis that flows from the types of shipments that have proven troublesome to us, where we found contraband. We take this historical record, run it through quite a large number of algorithms that sort, stack, rack and try to count in a very precise way and score in a very precise way that risk. That is the screening component.

Mr. DAVIS. Thank you.

I yield back.

Mr. JACKSON. I would just say, sir, we had none of this in any material way up to 9/11. I really am deeply respectful of the work

that CBP has done to make this work in this way. We can do better, and that is not to say that we haven't done a lot. I think that in our world, we are constantly pressing to make sure that we stay one step ahead of the bad guys. We can never rest with having done a good system and stop.

Chairman KING. I would like to recognize the gentlelady from California, who not only did such a great job in working on this bill, but also has become a proud grandparent. The gentlelady from California?

Ms. HARMAN. How much time do you have to talk about Lucy Asher Peck, Mr. Chairman?

[Laughter.]

Chairman KING. No filibustering. I know this would go on for days.

[Laughter.]

Ms. HARMAN. She lives in New York City, so there.

Thank you, Mr. Chairman, and thank you to all the members of this committee who have done such a good job highlighting and moving legislation on this issue. It is rare around here that the stars and the moon align so that we can move big bills. The last one I remember, at least that I was involved with, was the intelligence reform bill. I think this is going to be the next big one that moves through the House very quickly and moves through the Senate. I think when we are doing, we will have done something extremely significant.

I appreciate, Mr. Jackson, that the Homeland Security Department is working on many of these issues. However, I don't think you have gotten the job done yet, and we are going to push you a little bit by making certain that in our bill, which is still a work in progress, we have the right programs and the right amount of funding. I want to come back to that.

The subcommittee ranking member, Ms. Sanchez, said that she hoped that more good things would be added to this bill. I just want to note that the subcommittee, Mr. Lungren's and Ms. Sanchez's subcommittee, did add some more good things. The TWIC program, the TWIC language is critically important and so is Ms. Sanchez's language on third party validators. So I commend you. I am not a member of the subcommittee, but I commend you for doing that.

Now, at this level, I am excited about the fact that we will report to the full House what I think will be a strong bill. I am very, very proud to be one of the co-authors, along with Mr. Lungren.

Let me make a couple of points. First of all, Mr. Jackson, do you agree with me that at least up until now, between 9/11 and now, we have underfunded port security?

Mr. JACKSON. No, ma'am, I don't allow myself to jump to that word "underfunded." I think that we have been juggling massive requirements to put the country in the right order. The job is not done, as you said at the beginning. We have much more to do. That is why we have proposed a very significant increase in fiscal year 2007 to help on infrastructure for ports and for transit and other critical infrastructure.

Ms. HARMAN. Well, I believe we have underfunded port security. Just to take one little old port, the Port of Los Angeles, which with

the Port of Long Beach, is the largest container port complex in America. Almost 50 percent of our containers go in and out of those ports, and $26 million has been provided since 9/11. The request was $100 million. I can't vouch for every dollar requested, but my guess is that that funding level is 25 percent or so of where it ought to be to provide for real port security, not just for the residents, those who work in the port and the residents around the port, but for our country, given the fact that it is such a gateway.

At any rate, I hear you about the transportation dollars. I guess I just respectfully disagree. We have spent nine out of ten transportation security dollars, as I recall, on airport security, another huge area, but we have severely underfunded port security and that is why many of us feel strongly that we dedicated revenues for port security. The high-risk ports, whichever they are, should get those dollars. They should go for multi-year improvements and for things like this bill funds, which is a layered program for container security.

I know you support the thrust of the bill. I just hope you will get to "yes" on the whole deal because I think it has been carefully put together.

I want to ask a little about the ICIS project in Hong Kong. I know that numbers of senators and maybe some members of this committee, and Secretary Chertoff have visited it. It, I think, sounds like a very exciting idea. I am just wondering if you think that ICIS is some kind of magic bullet so that we can get to 100 percent of container inspection off-shore, hopefully in the next 3 or so years, which was an idea that was floated at the subcommittee level and which I still think is a valid idea.

Mr. JACKSON. I am very positive on the ICIS opportunity. We are very eager to take this to an additional step of implementation and work. There are a couple of parts of this that are particularly notable. One, this is a case where the industry, who have been valuable, valuable partners in this whole area of maritime security, have themselves stepped forward and said we are willing to tax ourselves to improve security. We should not lose that moment. It is a generous and right impulse to try to share the costs of making security work.

If we have that, and we could put in the in-bound lands in the overseas ports this type of rapid through-put, we could then multiplex the images, which is to say, electronically transmit them in real-time back to the United States for those containers that are headed to the United States, assess them if we have identified that container as a high-value target, a high-risk target. We could assess it instantly before it is loaded to help give additional data about it.

If there are some that we can assess on a random basis in a much more aggressive fashion, that type of tool, that type of framework over time would allow us to grow the amount of inspection that we are doing overseas. I think that we should move very aggressively here. I will tell you we are engaged in conversation with industry about just that and how to do it.

Ms. HARMAN. My time has expired, Mr. Chairman, but I strongly agree, and I hope "aggressively" means within 3 years.

Thank you. I yield back.

Chairman KING. I thank the gentlelady.

Mr. JACKSON. Better than that, ma'am.

Chairman KING. The chairman of the subcommittee, the former attorney general of California, Mr. Lungren?

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

Mr. Secretary, again I would like to go back to the screening versus inspection. As I understand what you just said, you said that the Hong Kong experiment is intriguing. It looks like the equipment they use at least can provide some additional information, and that it would be something that we might look forward to to have I thought you said 100 percent inspection from the standpoint of running the containers through one of these large machines as they come into the port. Is that what you were saying?

Mr. JACKSON. I think I tried to say, a very large number of inspections, but I avoided the word "100 percent." Let me just talk about that a little bit. I will give you an example, first, on the domestic nuclear detection work that we have. The plan that we have in place with the support from Congress and funding in our 2007 budget, would allow us to get to 98 percent inspection of all containers that have arrived in the United States and are leaving a port facility for radiological inspection.

Mr. LUNGREN. And that would be they would pass through this piece of equipment as they are beginning to drive out?

Mr. JACKSON. Yes, sir, before they depart the terminal. That is going to be using existing and a second-generation of tools which are much more robust and powerful, and which with the Congress's support we have been urgently pressing forward with the DNDO office on basic research.

Mr. LUNGREN. Is cargo leaving the United States?

Mr. JACKSON. No, it is leaving the U.S. port going into the United States. It is on port territory, but as it goes out. That is our objective.

Mr. LUNGREN. It is on the trailer pulled by the truck just before they would be able to exit the actual terminal?

Mr. JACKSON. Right. So why 98 percent? To go from the ports that carry that amount of through-put to get 98 percent, and then take the last 2 percent may be a disproportionate investment. So how would we work those 2 percent? We would probably use handheld devices, temporary mobile devices that would come and do a lockdown on a port and do maybe 100 percent in a given day, and then go to another small port where there may not even be a ship arriving every day, but on a periodic basis, so that we can work that last 2 percent.

I would say this is a reasonable tool so that we spend money based upon real return on investment. It is risk-based investment. Overseas inspections now, the ICIS program that Congresswoman Harman raised, is an inspection as a container enters into a port overseas before it comes our way, using the same types of tools. Could we get to 100 percent? Probably not without very, very severe imposition on both the industry and costs to the U.S. government.

But if we didn't inspect one of those in that way, and we have taken so much hay off the haystack, we could when it hits our ports have a much more intense look at the ones that didn't get

that type of in-bound inspection. None of them get it today. So we could in layers and over time bring much more discipline to that. I don't think that we have to say we will promise to be at 100 percent. What we have to promise is tough-nosed, hard risk-based analysis about how to spend the precious resources of the taxpayers here.

Mr. LUNGREN. One of the points I would like to make is, I have looked in vain to find any magic bullet. No matter what system you have, there are going to be shortcomings on those systems. It seems to me that we have to keep the emphasis on a multi-layered approach to security that includes the best technology applied, the application of intelligence, first of all the gathering of intelligence, but the analysis of that intelligence. We also need to have these algorithms and random inspections so that in fact we have a multiple attack on those who would attack us.

Because I just hope that when we talk about 100 percent of this or 100 percent of that, in reality there is never going to be 100 percent. We need to get the best technology we have and apply it as best we can, but always understand that we are going to have to have multiple layers so that we keep the other guys guessing. But also, we know that there are going to be shortcomings of any particular aspect of the system. It just makes sense for us to understand that.

The other thing I was intrigued about when we went to Long Beach–L.A. Ports, and went to the Maersk port, pier 400, where we saw what I was told is the largest ship that they have. It contains 8,000 containers. They are able to unload or load I think in a day-and-a-half. Someone mentioned that if you just added 2 minutes additional inspection of some sort, it might raise the time to 10 days.

So what I am suggesting is we need to be smart as to how we do these sorts of things. We need to understand the kinds of inspections we have, not that we shouldn't have inspections, but we have to keep in mind we are dealing with this commercial enterprise and how we do it is also important. We have to be smart about this thing.

Mr. JACKSON. I couldn't be in more agreement, sir. You have nailed it, I believe. It is a series of layered measures. It is not letting perfect be the enemy of good enough. It is continuous innovation, continuous commitment to reform. It is growing and growing, and it is the combination of all those layers working together that gives us greater security.

Mr. LUNGREN. I know my time is up. The only thing I am going to say, it is going to take money, though. I understand you put money on it, and I understand you have had grants. I don't think it is sufficient to have it just part of the $600 million you are talking about. That is why we are trying to dedicate a big chunk in this bill.

Chairman KING. The gentleman from Oregon?

Mr. DEFAZIO. Thank you, Mr. Chairman.

Mr. Jackson, always good to see you.

At home, our goal is to have 100 percent inspection of all containers as they depart a U.S. port headed into our country. Why is that? We think there might be a threat contained in those con-

tainers of some sort? Yes, would that be it? I mean, why else would we want to do that before they went inland? You must think there is a potential threat.

Mr. JACKSON. The threat is about risk and consequences and the intent to use these, the capability of using these as tools. So the consequences of a nuclear device being enclosed in a container is so high that it merits an unusual financial and physical work effort.

Mr. DEFAZIO. Okay. Now, that is once it has arrived in a U.S. port before it goes to a different large urban area in the United States. So are our ports then sacrifice zones? Why wouldn't we set this goal on the other side of the ocean? That is what concerns me. Mr. Lungren resisted this as an amendment last week. It sounds to me like you are saying technology exists. It is working real well in Hong Kong. They did it voluntarily. They are talking about expanding it. It could work. We could get to maybe 98 percent overseas. But in your testimony, it is our goal is to increase materially the number of containers inspected.

Now, we want to do 100 percent once they get in the U.S. before they go inland, so we think there is a risk of a nuclear bomb being inside, but we don't want to do 100 percent before they get to the port. Now, if I represent one of those ports, I would be real concerned about that. I might begin to change my position on whether or not we want to move this overseas if the technology has now been proven and say we want to set a timeline within which we want to have as near as practicable 100 percent. As you explained, we may not get to 100 percent. Wouldn't that be a reasonable goal?

Mr. JACKSON. Let me answer it this way for you, sir, rather than a yes or nor answer.

Mr. DEFAZIO. Be quick, because 5 minutes isn't very long. I have other questions.

Mr. JACKSON. Okay. The technology is not totally proven. We need to innovate more there. We need to do more testing. The technology that is taking these samples is basically going onto a disk and being stored.

Mr. DEFAZIO. Right. I know we are not reviewing it. I understand that. We have to hire someone to actually review it.

Mr. JACKSON. We would have to do that and we would have to get it over here. The next generation of technology has to be brought to bear.

Mr. DEFAZIO. Sure, a lot of fiber-optic capacity under the?

Mr. JACKSON. We can do this, sir. I am with you that this is not a technology barrier that can't be overcome.

Mr. DEFAZIO. Right.

Mr. JACKSON. Why did I say "materially" rather than "100 percent"? I think it is early enough to where we are entitled to be optimistic, but we should not be starry-eyed about understanding this with a layer of precision we haven't brought to the table yet. We would come back and tell you what percentage targets we would go for. We need more time to test whether this works and to make sure that before investing a large amount of money that it works.

Mr. DEFAZIO. But of course in Hong Kong, there was no U.S. investment and I understand they are willing to expand it to the entire port at no cost to the United States of America.

Mr. JACKSON. Well, it would have a cost to the United States of America to be able to staff and use their bulk operation.

Mr. DEFAZIO. Right, but I mean, that is pretty minimal, and we have had amendments to have more staff to review these things.

Mr. JACKSON. I am in agreement that it is a very generous commitment and we will try to explore this.

Mr. DEFAZIO. Okay. And then you said in this other testimony, which got a little confusing with the ranking member, but let me see. You said 100 percent were screened overseas, but in the GAO report they say here in the CSI ports alone, which are voluntary, cooperating, good people, that is 34 ports, we were able to target approximately 65 percent of the shipments to determine whether they were high risk.

So I am confused as to, and then when you go to the non-cooperating, non–CSI ports, it is a much lower percentage. So they say the total of containers coming in which we are able to actually target overseas is 43 percent, but you said they are all screened. So I guess that means we have a manifest on every one, but we haven't necessarily applied these additional measures that we are trying to do in the CSI ports, which we can do 65 percent of the time. Is that right, approximately?

Mr. JACKSON. What we have done is screen 100 percent of all inbound containers for risk.

Mr. DEFAZIO. "Screened" meaning we looked at a manifest.

Mr. JACKSON. We looked at it for risk and we have done the algorithms and the history check, and we have done that work. In the CSI ports, we are able to inspect with their cooperation a variety of cargo.

Mr. DEFAZIO. I am running out of time, but let me get to how you lower your score. My understanding is an overseas shipper submits paperwork, more than 10,000 submit it, and then sooner or later someone comes by to see that they actually have the security measures in place. We are told that they get their score lowered just by submitting the paperwork. In the Senate, they said 1,545 of 10,000 have been verified. No, the Senate said 27 percent. The GAO says 1,545 of 10,000.

So we have 8,500 shippers out there who have submitted paperwork and they get their score lowered. Now, don't you think that is pretty extraordinary? Wouldn't you say that really would merit putting a few more people on the job to actually at least go out once and see that al Zarquawi isn't there supervising the loading of these containers, at least 1 day when we come to inspect?

Mr. JACKSON. Let me tell you how it works, and the answer is we do need to do more validations is the punchline here. We have about 5,800 businesses, which account for 45 percent of all imports. I think that was the 45 percent number that you were talking about. Of those, 27 percent have been through a completed validation.

Mr. DEFAZIO. What was that? I am sorry.

Mr. JACKSON. About 27 percent of the 5,800 businesses have gone through a completed validation, and 65 percent will be completed by the end of 2006, with the assets that we have in the pipeline. So we are trying to accelerate those validations. That is why I think the idea presented by the committee of third party valida-

tions is also a valuable one, so that we do it once, we do it again, we go back, we have some baseline that we keep checking.

This didn't exist at all. I have to give a lot of credit to Rob Bonner. We have come this far. We have to go farther.

Mr. DEFAZIO. Thank you.

Thank you, Mr. Chairman.

Chairman KING. The gentleman from New Mexico, Mr. Pearce?

Mr. PEARCE. Thank you.

Thank you, Mr. Secretary, for your presentation.

The cargo screening, does it work if the radiation sources are lead-shielded?

Mr. JACKSON. There is a certain amount that I would rather talk about in a non-public hearing that can get into classified information. But at a high altitude with open-source data, lead shielding presents one type of problem, or shielding presents one type of problem, and we use multiple tools to find those problems or those efforts.

Mr. PEARCE. You mentioned on a combination of page one and page two about a lot of your work is going into the global nonproliferation, making weapons components more difficult to acquire. Exactly what are you doing there and how much more difficult is it?

Mr. JACKSON. Well, it is a challenge to try to work on nonproliferation issues. It is not principally a Department of Homeland Security task. It is a State Department and Defense Department and Energy Department, other efforts. In ports, to give you one example, the Department of Energy has the so-called Megaports program where they deploy radiation detection equipment at foreign ports and then help train foreign governments to look for radiation. This is not all about screening things headed just to the U.S., but it is about trying to make sure that all countries are putting a priority on this.

There are multiple components to the nonproliferation that we have, which is deconstructing nuclear weapons, making sure that we tag inventory and monitor the repositories that contain nuclear materials, the various security elements associated with protecting and managing the production, the storage and the movement of nuclear materials.

I would be happy to provide considerable more detail is that would be helpful to you from an interagency perspective.

Mr. PEARCE. You refer to the ATS as being an extraordinarily powerful tool. It computes the algorithms and things that I don't know much about. It seems like that one of the threats of terrorism is that people tend to go underground and they operate for years in cells, and then they simply come out when needed. How does your algorithm process, anticipate those risks from sources who have not previously been identified and who haven't yet been activated?

Mr. JACKSON. It is an excellent question. It is an enduring security focus. There are multiple ways to tackle that problem. First, in the risk-scoring, there is an element of randomness in all security programs so that you can't get a free pass every day, every way just because we think that on the whole you are lower profile.

Second, this is all about the layered security work that we do, some amount of random inspecting virtually all containers as they leave, for radiation, for example, is a trust-but-verify tool; working with our counterparts from foreign governments to do physical inspections overseas. For example, we had a problem with some individuals smuggled in an empty container. We then worked with the firm that was affected and the country that was the origin of this shipment, and have put in place a multiplicity of tools to look at the empty container issue.

So it is a constant press to innovate and to look and to take multiple different tools, some physical, some cyber analytic tools, but to focus on these issues so we do not have a predictable way to circumvent this scrutiny.

Mr. PEARCE. On the budgeting, the numbers of the bill, section 14, joint operations centers is $100 million. I am not really seeing a very thorough explanation of exactly what that means and implies. I see a grant process that is R&D related, but can you explain that just a little bit?

Mr. JACKSON. That was not per se an administration figure or number. We in principle believe that the idea of connecting virtually and physically the various components that are doing assessments is important. We have not proposed that type of investment and would need to do some further analysis about what we would recommend by way of missing appropriations or additional appropriations in that area.

We have centers, for example the Coast Guard does. It is profiling its review of in-bound vessels and mariners at a facility in Maryland. CBP's excellent facility to do the container profiling piece of this is done in Virginia. Those two connect very, very seamlessly in the passage of information back and forth at various points along the supply chain, and our work with them.

So we have to continue to work and improve those capabilities, but we don't necessarily have to co-locate physically to make that happen effectively.

Mr. PEARCE. Thank you, Mr. Chairman.

Chairman KING. The gentlelady from the Virgin Islands?

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

I want to welcome the secretary and also commend our colleagues for the SAFE Ports Act. I am glad to be a cosponsor of it.

Of course, now that it comes to me, many of the questions that I wanted to ask have been answered already, but I wanted to just underscore that like my colleagues, my constituents are very concerned with the short staffing and the lack of adequate staffing in Coast Guard and Customs and Border Protection, and of course the lack of a border patrol, which would help us to help our nation prevent attacks before they get to our shore. We cannot do that right now.

We want to work with you. I have the support of my chair and ranking member on this to rectify that deficiency in my area of the world. We also still have those concerns with the advance passenger information system program. We are working with your department and would like your support in working to alleviate some of the triplicate requirements that our charter boats have.

Last week, I guess it was, Secretary Jackson, the port security expert and former Coast Guard Commander Stephen Flynn testified that the Maritime Transportation Security Act regulations are a sketch, rather than a security blueprint, and that it sets forth general requirements that are not well defined. He stated, for example, that the requirements require safety security plans, but do not define what "security" is; that they require a qualified individual to implement the security actions, but do not define what "qualified" is.

I know that all ports are not the same and that the regs therefore were issued to be very broad, but after the events of the past month or so, has the department looked into the possibility of tweaking the regulations to give ports guidance of what is required of them? In our case, we have some very small ports that are within the Virgin Islands that perhaps also need some tweaking for their unique situations.

Mr. JACKSON. First of all, let me say that we would be happy to entertain a discussion about any particular points of rub in the security plan as related to the Virgin Islands, and I would be delighted to have the Coast Guard work with you on that and CBP on that issue.

As a general rule, Congress has given us a broad architecture and framework. We bring that down to a more specific level with our regulations. You are exactly right that we cannot anticipate every single plan in those regulations. The cornerstone of this tremendous MTSA authority, the maritime security bill's authority, is to give the captain of the port the capacity to make these adjustments and to focus within the port community, public sector, private sector, the federal agencies, to make a workable plan, and then to push it and to understand it and to test it, and to gauge its success.

This is, again, a work in progress. I think we have made tremendous progress in this area. Is it perfect? Nothing is going to be perfect and we are committed to continuous innovation here. But I think that we have with the regulation, and then the concomitant authority exercised through the captain of the port, a very strong capability to get very granular and to get very specific and to be very precise in how we improve security.

Mrs. CHRISTENSEN. Thank you. I really don't see the need to ask a question about this. I would just want to sort of underscore what was said before about the dissatisfaction I have with the APS system as well, and my concern that it really is not what we need in terms of cargo security, and say that I hope as we and the department look at the ICIS that the secretary looked at last week, I guess it was, in Hong Kong, that you will help us to help you to make sure that we can move as quickly as possible to get to that 100 percent inspection that will make all of us a lot more comfortable.

Relying on reports and written statements as to what is in a cargo and despite the fact that it is all coordinated and you try to come up with as specific as possible and as targeted as possible ways to look at what the manifest says and the container, there is a lot of discomfort with that still. There have been times when the department has not really relied on the committee to be the kind

of support that we are here to be for the department. We want to make sure that the funding is available and whatever authorities are necessary are there to ensure that we can move to 100 percent of cargo inspections as soon as possible.

Mr. JACKSON. We welcome very much that spirit of cooperation. Mr. Chairman, I would just make the invitation that for any members that would like to come out to our targeting center and see a demonstration of this layered security profiling work that is done for containers, we would be more than happy to make a time for members and staff to see this in more detail. It is a substantial tool. We need a layered system of multiple tools to answer the mail.

Chairman KING. I will be taking you up on the offer.

Mr. JACKSON. Yes, sir. I would like to go with you when you want to go. It is quite a tour and something that really is provoking of deep reflection on how best to move this.

Chairman KING. The gentleman from the state of Washington, the chairman of the Emergency Preparedness Subcommittee, Mr. Reichert.

Mr. REICHERT. Thank you, Mr. Chairman.

Welcome, Mr. Secretary. First, I want to say thank you personally. You have been very responsive to my requests. In fact, you have initiated two or three phone calls to me personally as the new chairman of the Emergency Preparedness Subcommittee. I appreciate your open communications style and your willingness to work with me and members of our subcommittee.

Mr. JACKSON. Thank you.

Mr. REICHERT. I want to touch on, I know there is a layered approach in many different ways as you look at port security. In the organizational structure, too, I know that section 14 of this bill seeks to create a maritime security command center. As the sheriff in Seattle for a number of years, we participated in the joint analytical centers and the JTTFs. I am just curious as to how the maritime security command centers, JTTFs, and joint analytical centers, how that layered approach, how they interact with each other and work with each other.

Mr. JACKSON. In various different ways. The JTTF model has been in a specific tailored way replicated, for example, in San Diego, where they physically have created a fusion center where federal, state and local officials are co-located and work very closely with each other on the maritime domain awareness issues and on the law enforcement issues associated with port security.

That is not the only model that works well. We can create a common operating platform, a COP, that can be shared virtually, and we do rely on the JTTFs in our port areas to work with the law enforcement community especially closely to work on port security issues. So it is information exchange. It is sharing it across the wide body of people that need to know it. It is making sure everybody is in the family and talking together. It is using that captain of the port to be the central point of focus.

Mr. REICHERT. That was my next question. The captain of the port, which is a member of the Coast Guard, how will they now interact with the director of cargo security?

Mr. JACKSON. The captain of the port works very closely with the cargo security officials in each of the terminals and the terminal operating companies, with the port director, and with the ocean carriers moving cargo through the port, with the rail and truck community that is moving in and out, and with the broader set of actors that are moving commerce. There is a port security committee that is formed in each of our ports that manages these issues, that exchanges routine information, and that provides a single point of focus for getting a game plan together for the port.

Mr. REICHERT. Who is a member of the joint analytical centers? The captain of the port?

Mr. JACKSON. The captain of the port and it depends, the law enforcement community has access to analytical data, and then as appropriate, the industry as well, and it is oftentimes very appropriate for them to be cleared in, let in, and to have access.

Mr. REICHERT. One of the things that I am hearing concerns about from employees at our ports in Seattle and Tacoma, Washington is they are very concerned about the training that may or may not exist in some ports across this nation. Do you feel there is enough attention that is placed on the training and exercises? Who has the ultimate authority over the planning of the training and the exercises? Is it the captain of the port? Is it the cargo security director? Who really is in charge?

Mr. JACKSON. It is somewhat diffuse, and that is probably not a perfect circumstance. We have federal exercises. We have federal grants for exercising and training. We have law enforcement-related grants for some of this work. We have state grants for others. Sometimes, the military when, as in your area of the world, has significant assets, they bring training and exercise work to the table. So there is honestly a variety of different points for managing that.

We are trying to consolidate that within our new preparedness directorate at DHS so that we can have one broad picture of who is doing what, and try to make sure that we are being as helpful as possible in stimulating the right work.

Mr. REICHERT. What role do the owners of the port terminals play in port security?

Mr. JACKSON. They play a very important role. The terminating operating companies typically, as is the profile in your area, a municipal authority or a state authority would own the port itself and the terminal operator has a long-term leasehold. The operators of those ports, which sometimes are ocean carriers and sometimes are firms that are created just for this purpose of operating a terminal, are indispensably connected to the security plans. The have requirements under the law and they are part of the port planning.

Mr. REICHERT. So the Japanese owners, the crane owners of these companies?

Mr. JACKSON. They are at the table. They have requirements. We measure, manage and hold them to account.

Mr. REICHERT. Thank you, Mr. Chairman.,

Chairman KING. The gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman.

Mr. Jackson, in the subcommittee last week by a party-line vote on my amendment, which required 100 percent of all boats containing cargo coming to the United States, would be screened before they reached the United States. That vote failed by an eight-to-six margin, with all six Democrats voting to screen all cargo before it gets to our country, and the majority of the Republicans voting not to.

Now, your testimony here today indicates that that is the position of the Bush administration, that the Bush administration opposes the screening of 100 percent of cargo, the screening of 100 percent of cargo which comes into the United States. Is that correct, Mr. Jackson?

Mr. JACKSON. No, sir, that is not correct.

Mr. MARKEY. Does the administration favor the screening of 100 percent?

Mr. JACKSON. Yes, we do, but I think in fairness I need to make a distinction here, which I think Mr. Defazio?

Mr. MARKEY. Do you favor the physical inspection of all cargo coming into the United States?

Mr. JACKSON. Not at this juncture. We don't have the equipment and the capacity to manage that. I think that would throw out of whack the balance between mobility and security.

Mr. MARKEY. Okay. So the administration opposes the physical inspection of all cargo before it hits our shores. Is that correct?

Mr. JACKSON. We do not have the current tools and capabilities to achieve that objective.

Mr. MARKEY. Are you saying the technology does not exist, because in the Port of Hong Kong they have the technology which makes it possible for them to physically inspect all cargo?

Mr. JACKSON. You are speaking, sir, of the ICIS program, and I am very encouraged. As I have testified earlier in this hearing about the ICIS program, but the ICIS program has multiple technological steps and refinements that need to be pursued in order to make it an operational tool.

Mr. MARKEY. So according to the industry witnesses, it would cost only about $100 to inspect physically each container before it comes to our country. When you compare that to the $66,000 average value of goods in each container which comes into our country, we are talking about a cost increase of .02 percent. Is that really too much to ask, Mr. Jackson, in order to ensure that a nuclear weapon has not been smuggled into our country on one of these ships?

Mr. JACKSON. As I have testified here earlier today, sir, I am very encouraged that we can get a very, very high amount of screening and also, well, 100 percent screening, and also a very high amount of inspection through these types of tools and through this type of innovation. I believe that we are not there today with the tool kit, but we should and are moving very aggressively to try to explore how to make this happen. It is not something that we are sitting on our haunches about. We are actively working it.

Mr. MARKEY. You are actively working on it, but you are rejecting both the Republicans in the Congress and in the Bush administration is rejecting 100 percent inspection of cargo.

Mr. JACKSON. No, sir. We are talking about what is practical in the world that we live in today.

Mr. MARKEY. Well, I appreciate that, but you could argue that it is not practical to screen every one of our bags that goes on airplanes, and some people argue that. But I don't think any American wants to go on a plane that doesn't have 100 percent of all the bags that are going on planes to be screened, do you think?

Mr. JACKSON. I think they do, and that is why we screen 100 percent of bags.

Mr. MARKEY. Exactly right. I think Americans also want 100 percent of all the cargo which comes into our country to be inspected as well, in view of the fact that these nuclear materials, as you know, are all over the former Soviet Union, can be purchased potentially and put on one of these boats and brought to our port, and we know that al-Qa'ida has designed this nuclear event in our country as their highest goal. So why wouldn't we make that our highest goal, to block them from being able to accomplish that goal?

Mr. JACKSON. That is what my testimony says at the very outset, which is that weapons of mass destruction is the administration's highest priority, and then we have to take it, sir, in a deliberate way to unpack the component tools that we can use to be able to find any potential weapons of mass destruction that are secreted in a container. There are multiple layers, some of them occur overseas, some of them domestically. I have said, and the administration is strongly supporting in the U.S. to have 98 percent of all outbound containers leaving a U.S. port into a community screened with sophisticated nuclear detection tools by the end of next year. We have made tremendous progress so far.

The ICIS program, which I believe you are discussing, presents I think a terrific opportunity for us to leverage a commitment by the industry to bring nuclear detection capabilities overseas to ports that would allow us to inspect with these tools in-bound containers into the United States.

Mr. MARKEY. What you are saying, Mr. Jackson, is that the Bush administration does not want to impose a burden on the cargo industry; that the Bush administration doesn't to impose a burden on the shipping industry. This whole attitude that the Bush administration has of "in industry we trust," for chemical, for nuclear security in our country, just pervades these wide-open loopholes that have been allowed to be maintained.

By not making a goal to have the incoming cargo have the same level of scrutiny which you are saying that outgoing cargo is going to have in the U.S., gives al-Qa'ida an opportunity to plot to bring the nuclear weapon in on a ship into an American city to create this nuclear event. It is too dangerous, Mr. Jackson. It is too risky, knowing that they have put it at the top of their terrorist target list.

Chairman KING. The time of the gentleman has expired.

If the secretary wants to respond, he can.

Mr. JACKSON. I will just respond briefly that we are focused on this threat vector in the most intense way. What we are using is a multiplicity of tools starting with our screening of 100 percent of all containers that are coming this way. We are taking physical in-

spection tools abroad and domestically, some when they get off the ship immediately; some when a ship is boarded at sea before it comes into a port.

When we find a container that we believe is a risk, we inspect 100 percent of those containers. So it is not one silver bullet that solves the problem. It is multiple tools. It is not one thing that can be done today, but it is a commitment to grow and innovate and strengthen the security of the system.

Chairman KING. The gentleman from Alabama, Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman.

Thank you, Mr. Jackson, for being here.

I want to talk about port security personnel.

Mr. JACKSON. Yes, sir.

Mr. ROGERS. Specifically, last week in subcommittee there was a proposal to raise the number of port security personnel by 450 per year. My question to you, first, is, what is the level of port security personnel that we have now? What is the desired level, in your opinion, in the next year and then over the next 5-year period?

Mr. JACKSON. Mr. Rogers, if I could get back to you with the exact figures, I would be grateful. We need to break them down into four groups: the Coast Guard people domestically; Coast Guard people doing port security analysis overseas. Those are two. And then we need CBP people here domestically, and CBP people overseas.

There is an overlay for this which is part of the security plan, of the captain of the port imposed security plan that the local community provides, the local law enforcement, and then also that the operators, either the terminal operators, the ocean carriers or others, are required to bring to the table.

It is that combination of all those assets to get to the personnel question. Let me try to be just candid. I think that we are using significant assets here. It is true that you can always pour more people at these problems. I think the prioritization issue, and I talked about the new commandant-to-be of the Coast Guard just as recently as this morning, it is to focus on those types of attacks that we think are the highest vulnerability.

We can't afford simply to fund every good idea. This idea you are raising is an important idea. It is an idea that I am not dismissing by any stretch. I think that it is possible that we can use more people to accelerate our review work, and then we are going to have to just balance the dollars and say, where should we spend, what do you think, what does the Congress believe is the right balance on these tools in the tool kit to fund.

Mr. ROGERS. Don't get me wrong. It wasn't my proposal to raise it by 450. It was raised. The reason I suggest that proposal, my question was, how will we train those Border Patrol agents and absorb them? I looked to the Border Patrol training problem we have now. As you know, nearly 18 months ago, 10,000 Border Patrol agents were authorized, and to date, almost 18 months into that period, we have a little over 500 that have been trained and put in the field, solely because we don't have the capacity to train more than we are training with our current infrastructure, and absorb them.

In fact, CBP officials have told us that even if they had 2,000 per year trained, they physically could not absorb that many Border Patrol agents in the field. So my question is, if we were to need, in your opinion, after you review the process, and I would appreciate you letting me know your opinion after you have looked at your facts, how many new port security personnel you need. Where would they be trained? And what numbers per year? How much would it cost us to train them? What kind of training do they need? Do you know off-hand where those port security personnel would be trained?

Mr. JACKSON. It depends on which ones we are talking about. The Coast Guard at their facilities train their people to do this MTSA Act inspection and auditing work, and CBP has different facilities for theirs. So they are done in different places. I am very well aware of the gating limit on Border Patrol training at about the level of 1,500 per year, which is what we will put into the field this year with the Border Patrol.

Mr. ROGERS. I am thinking specifically about our seaports.

Mr. JACKSON. Yes, sir.

Mr. ROGERS. Where are those personnel trained?

Mr. JACKSON. I would have to ask. I will have to get back to you on that, sir.

Mr. ROGERS. If you would, and what the cost would be, and what you think with our current infrastructure the number per year that we could train would be. I would appreciate that.

Mr. JACKSON. Yes, sir.

Mr. ROGERS. Thank you.

Thank you, Mr. Chairman.

Chairman KING. The gentleman from New Jersey, the ever-dynamic Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman.

Before I ask my questions, I would like to ask the under secretary, the committee has been asking for an organizational chart of DHS for months now, and can you assure me that we are going to get it by the end of the week?

Mr. JACKSON. I will give it to you tonight, sir. It is one that I can show you.

Mr. PASCRELL. Thank you for a quick answer.

Let's start off with an easy one. In the aftermath of the Dubai Ports dispute, I am somewhat weary of the administration's hiring of Hutchison Whampoa, a Hong Kong-based company with close ties to China, to help detect nuclear materials inside cargo passing through the Bahamas to the United States and elsewhere.

Now, in fact Clark Kent Ervin, who is going to be testifying in a little while, he was the first Homeland Security inspector general, and has stated that the $6 million contract given could compromise U.S. homeland security. Now, I understand that the Department of Energy is going to finalize this contract.

I would like to know the following: What level the DHS has been involved with in this process?; secondly, to what extent can you assure the committee that all security concerns have been addressed, and in particular whether or not we have or will have in the future CSI inspectors on the ground at this particular fort? Mr. Under Secretary?

Mr. JACKSON. Yes, sir. Let me explain what this contract is. It is an Energy Department Megaports contract to put radiation detection material in the Bahamas port. The machines are in this particular configuration in this port, not fixed portals that you drive things through, but rather they are incorporated into the so-called "straddle" carriers, the machines, the trucks that move containers from one point to another inside of a port.

That equipment is an agreement to manage that equipment, to run that program, is a government-to-government commitment, not a commitment with the terminal operating company, the Hutchison–Whampoa.

Mr. PASCRELL. A government-to-government?

Mr. JACKSON. Yes, sir.

Mr. PASCRELL. Which two governments?

Mr. JACKSON. The Bahamian government. So the machines are on equipment that is run literally by a terminal operating company, but when the machine is turned on, it cannot be turned off without the monitoring service, which is the government function there, knowing about it. The signal about radiation detection goes to the government agency.

The operating company does not manage the resolution of these alarms. It is not responsible for the resolution of the alarms. It is not responsible for the protocols of detection. It is not responsible for the program. It is simply part of this process that is used to be able physically to get a container to a point where it can be inspected with this device.

Mr. PASCRELL. Will we have our own inspectors in that country?

Mr. JACKSON. We are working closely to a CSI designation for this port. I am told that CBP is confident that we will be there shortly.

Mr. PASCRELL. I think that would be critical and answer a lot of our questions that we have concerning this particular deal. We have a lot of questions in many of our minds.

I want to get into the budget right now, okay, if you will. For fiscal year 2007, the Department of Homeland Security requested $600 million for the targeted infrastructure protection program, a unified, non-mode-specific security grant program. However, over the past 4 fiscal years, the Appropriations Committees have provided mode-specific funds for transportation security grants, breaking out port, transit, rail, intercity bus security grants as separate budget line items.

What was the reasoning behind having ports and transit and rail buses and highway watch programs compete against each other for security funding? Or in your words, why are we bundling this when each of these areas are categorical and have their own unique entities?

Mr. JACKSON. The principle is to allow the local authorities and the owners of this infrastructure to be able to present the highest risk threats and to allow us to fund the highest risk treats. If I could just go back to last summer when the London transit attacks occurred, many of us in this room were focused quite intently on how to strengthen the transit security needs that we had.

If we could give some flexibility to do transit or port, we could I think give ourselves a greater degree of focus on the highest

risks. It is not a simple equation to figure out which is the greater of the competing demands to improve security. We are saying with this program we are making our state partners a much more active partnership than us making these priorities.

Mr. PASCRELL. Mr. Chairman, in conclusion, I just want to enter for the record, I think that this is the wrong way to fund these programs. They are competing against each other, and we will never get to the point of reflecting the emphasis and priorities of this committee.

Thank you.

Chairman KING. The gentleman's remarks are so noted. I would point out that in the legislation which is going through the committee, we are segregating out money for port security.

With that, the gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. Secretary, thank you for your testimony and your time here today. Let me quickly get to some questions on container security. I understand that you have 42 offices open now worldwide on the container security initiative. My understanding is you plan to expand to 50 by the end of this fiscal year. However, a recent GAO report states that the program is experiencing staffing shortages in the offices you have, of the 42 you have now in existence.

We have also heard reports that some foreign port operators have been subject to only cursory inspection before being named CSI sites, despite Customs Border Protection and the Coast Guard and the State Department receiving outside information that corruption and fraud at these sites exists.

My question is, how do you decide where to locate a CSI office? How do you assess the port security capabilities and their vulnerabilities? And thirdly, do you require the port management authority to address security concerns before opening an office?

Mr. JACKSON. Yes, sir, let me try to answer some of those questions as best I can.

How do we assess? We use multiple different tools. One idea that is a driver of CSI is that we are trying to move to capture the largest amount possible of in-bound containers into the U.S. So at one level, it is the Willy Sutton model. We go where the money is. Here, we go where the containers are. We are looking for the big load-out ports that are moving the vast bulk of traffic in here.

Right now, we are counting through CSI of about 75 percent of the in-bound traffic. By the end of the year, if we get to our 50 goal, we will be covering about 80 percent of the in-bound traffic. So the first screen on that is where are the containers coming from.

A second screen is that we look at multiple security tools. You are absolutely asking good questions, fair questions. The Coast Guard has an overseas program of port inspections. We use those tools. The Customs Service also does their own assessments. We have detailed conversations with the government where we propose to start this. We also assess the private sector as part of that work.

So it is a series of different screens and tests to try to figure how best to target the CSI ports.

Mr. ETHERIDGE. How do you verify the progress? You do it initially, but how do you verify the progress as you move along? Do you have a place for quality control?

Mr. JACKSON. It is a good question. I know I don't have all the answers to it, and I would be happy to get some more granular information.

Mr. ETHERIDGE. Would you?

Mr. JACKSON. Yes, sir.

Mr. ETHERIDGE. Because I think that is critical in this area.

Mr. JACKSON. Yes, sir. I agree.

Mr. ETHERIDGE. It is one thing to open an office, but if you aren't going to verify it and monitor the progress—One final point I would add in this area before moving to another one is that we hear a lot about technology. I am a great fan of technology.

Mr. JACKSON. Yes, sir.

Mr. ETHERIDGE. But it seems to me, having personnel on the ground gives you intelligence that you will never get from technology.

Mr. JACKSON. Agreed.

Mr. ETHERIDGE. If the personnel aren't there and we have opened an office, I think we open ourselves up to feeling good about having success in inspections, when really and truly we may be lulling ourselves to sleep for a problem.

Mr. JACKSON. If a CSI port is not staffed with CBP personnel, then we are not operating as a CSI port. We may have vacancies or shortfalls in moving people overseas. It is quite expensive and a time-consuming process to get people transferred to an overseas assignment and there. So there is some natural amount of turnover, but a corps of people running the program is indispensable and sir, I agree totally that that human-to-human contact where you can see it with your eyes and work with the people on the ground from our counterparts in CBP overseas is an indispensable part of the layered system of security.

Mr. ETHERIDGE. All right, since you raised that issue, let me go a step farther then. How do you intend to handle the existing shortages? What plan do you have in place to deal with those, plus for those you plan to open an new office, because you have to have people to fill the vacancies when they come up and to make sure you have them. That is critical, it seems to me.

Mr. JACKSON. Yes, sir. It is a staffing plan. In response to your question, I would be happy to get some vacancy analysis done and show you where we are with this. It is a commitment of the CBP leadership and DHS to make sure that we are adequately staffing the CBP program overseas for CSI.

Mr. ETHERIDGE. Would you? I think this committee would like to have that information.

Mr. JACKSON. I would be happy to give it to the committee.

Mr. ETHERIDGE. I think that is a critical issue.

One final question, we are now dealing with legislation, and if Congress should provide the additional funding for DHS beyond the budget request, with all the stuff we have heard on port security need, if we should do that, how could you best utilize these funds to improve port security, in your own words?

Mr. JACKSON. There are a couple of high priorities that I identified in my testimony that I would use money for first. The secure freight initiative, which gets us a greater capacity to get the next generation of targeting capacity merits money. We are reprogram-

ming if necessary and reassigning money as possible to try to launch that in an effective way this year. If we need more money, we will ask for that because that is an indispensably high priority.

The second area that I would mention is the area culled out of my testimony about next generation detection tools. If we can leverage the work that the ICIS experiment shows us, that might require us to assess our future budgets. It is not a plan that is fully baked now, but if we could get to something there that required additional expenditure or the reallocation of assets within DHS, that would be a priority for me.

Third, I would say the TWIC program is a very, very important priority for making sure that we have fully funded. We have a path ahead identified inside the department about what we need for the rest of this fiscal year. We may need to come back and assess whether we should reprogram, reallocate or reassign money in some way or another to make sure that when we implement it fully in the coming year, we are adequately funded for that.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Thank your indulgence. If I could make just one point on this. I would hope that as you share with us information between technology and personnel, as you are looking at these things, I would like very much to see, and I hope you will share with the committee, the issue of personnel on the ground for intelligence. I think this is an issue that we have a gray area that we need to have covered, and I would like to see that, if you will please.

Mr. JACKSON. Yes, sir.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Chairman KING. I thank the gentleman.

The gentleman from Rhode Island, who has been particularly active on the issue of radiation portal monitors, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Mr. Secretary, I want to thank you for your testimony today. I enjoyed reading the testimony and I will have additional questions for the record. But just briefly, I would like to begin with, you referenced DHS's plan to expand the number of the radiation portal monitors and next generation advanced spectroscopic portals. A GAO study last month indicated that DHS is 5 years behind schedule to deploy more than 3,000 RPMs by 2009, and the program is underfunded by more than $300 million.

My question to you first is, will you come to the Congress to ask for immediate funding so that the program can be completed as soon as possible?

And next, a Senate report showed that less than 40 percent of cargo entering the country is screened for radiation. We have had an active discussion her already about screening cargo, but can you tell me what factors limit the rapid deployment of RPMs so that DHS can meet its goal of 100 percent inspection of cargo at our ports?

If you can take the budget one, though, on the deployment of RPMs and the fact that DHS is behind schedule, I would like you to address that one first.

Mr. JACKSON. I would say that we are actually not behind schedule and that we have made very, very substantial progress since Secretary Chertoff has come into office. It was one of his very high

initial priorities to explore this area. We have, with the Congress's help, funded the domestic nuclear detection office, the DNDO. The DNDO is aggressively working with CBP on the deployment of radiation portal monitors and the next generation of these RPMs.

We have a very accelerated, aggressive, and I am telling you very promising procurement underway for this next generation of tools. We have been testing them in conjunction with the national labs where we have actual lab tests that are showing great promise. So we have a plan. The plan started predominantly with our land border crossings for this deployment, where we saw the immediate need to be so high. We are moving very rapidly into the maritime world.

Right now, we see containers subject to RPMs, radiation portal monitors, at slightly over 50 percent right now. So we have seen, even when I first testified in the middle of the Dubai Ports World, this was lower by five or six points. So we are now in the very active phase of bringing every month substantial capacity online. I think that we will get to the goal that I mentioned of the 98 percent deployment of all containers screened by the end of fiscal year 2007.

We have asked for a very large amount of money for DNDO, and the Congress so far has been very supportive. If we feel like we need more, we will come and ask you. So that is the budget part of that equation.

Mr. LANGEVIN. If I could ask, in terms of follow up right there, if you had the additional money now, though, isn't it true that you could accelerate the deployment of those border monitors at border crossings in our ports right now?

Mr. JACKSON. I would have to go back and look at the question of whether we can push the supply chain faster than we are. We are buying very aggressively. One part of what we have looked at is there are certain components of these machines that we would like to see available in a more rapid turnaround. We have looked internally about how to provide incentives to industry to make sure that those components are available so that we could accelerate into the next generation as soon as the technology is refined.

So I don't now for sure whether we are buying up everything on the assembly line, and if the assembly line is working at maximum capacity. I know that we are buying a very considerable amount and that we have invested people and the dollars to do it as fast as possible.

Mr. LANGEVIN. Mr. Secretary, would you get back to us with the answer to that question? Because it is my understanding that it is within our capability, it is within DHS's capability, that if you had the funds, that you could deploy the radiation portal monitors at all of our borders, ports of entry, ports within 1 year. Actually, I had, with the help of this committee, passed an amendment that would have required the deployment of these radiation portal monitors within 1 year.

It really is my understanding that it is a budget function, and it is a very small amount, approximately about $130 million over what the president has requested for radiation portal monitors. It would get the job done. I think it is both shortsighted and it is irre-

sponsible for us not to appropriate and authorize that additional funding if it is that small amount of money.

In comparison to what we are spending in Iraq on a daily basis, another $130 million is a small amount, in comparison to what it would do and what it would give us in terms of protection based on the threat.

Mr. JACKSON. I would be happy to give you some production capability figures. I will tell you that in response to a discussion of the amendment that you raise, I was briefed by my staff that we thought that there were production limits that would prevent us from meeting that even if money was not the issue. But I would be happy to provide a little bit of additional detail to unpack that assessment from our team for you, and let you know more detail about why they have that conviction.

Mr. LANGEVIN. I would appreciate that.

Mr. JACKSON. Yes, sir.

Mr. LANGEVIN. With the chairman's indulgence, if you could just brief answer the last question, that was what are the limits on the rapid deployment of RPMs so that DHS could meet its goal. Are there technical things that you can point to?

Mr. JACKSON. I think the issues are money, as you have identified, and the technical production capabilities. There is also a third element that we are very mindful of, that we see just around the corner in the near term, some potential dramatic breakthroughs in the technology. So we are trying to make a balance here to say, how would you weigh the full-bore, spend all the dough, get it out as fast as possible, with a piece of technology which is now going to be replaced by a much more highly functioning piece of equipment? So we are trying to cover as much of the mass as we can, have layers of security in the interim while we move to a new technology.

If this were pie-in-the-sky or we thought that it may or may not happen, that balancing act might have a different equation. But because we are so convinced that this next generation of radiation monitors, which will allow us to understand the particular types of radiation signal that we are getting, is around the corner and is possible, we are trying to balance those type of capital investments so that we have a long-term tool that will be satisfactory for the country.

Mr. LANGEVIN. Thank you. I know my time has expired, so I just wanted to end by saying that let's keep in mind, though, let's not let the perfect be the enemy of the good; that there will always be the next best technology out there; and from what I understand what we have right now on the market is good enough to do the detection that we need to do. There will always be better equipment, but let's not let the perfect be the enemy of the good.

Mr. JACKSON. I understand. That is a valid principle.

Mr. LANGEVIN. Mr. Chairman, thank you for your indulgence. I appreciate that.

Chairman KING. The gentlelady from Texas?

Ms. JACKSON-LEE. Thank you, Mr. Chairman. Let me personally thank you as well for your courtesies of last week. I appreciate it very much.

Mr. Jackson, welcome. Let me thank you for your service. I have been known on this committee to be pointed with respect to my belief in some of the responses given by the Department of Homeland Security. I want to personally thank you for your leadership on another matter dealing with the aftermath of Hurricane Katrina, and specifically dealing with what I call the impact states.

As you well know, we are still feeling it. You may hear from the city of Houston again for a number of issues, including housing, and maybe your collaborative efforts with the Department of Justice on security, I know that they are the ones that are handling that funding, but I do want to thank you on that.

Mr. JACKSON. Yes, ma'am. Thank you.

Ms. JACKSON-LEE. You are quite welcome.

Do you have any assessment of the status of the Port of New Orleans at this time?

Mr. JACKSON. I don't have a particular security assessment. I do know that we have brought back the port to operational capabilities of a core nature. There are still some considerable damage and limits on the capacities in the port.

Ms. JACKSON-LEE. I would be interested if I could get a report on the functionality of the port at this time, separate and apart from security, but adding to that what is its security status.

Mr. JACKSON. Yes, ma'am. I would be happy to get it to you.

Ms. JACKSON-LEE. I say that because my questions will be intertwined with the vulnerability of ports both in terms of manmade disasters, terrorist acts, but also what we saw, the catastrophic event of Hurricane Katrina, and to a lesser extent Hurricane Rita.

As you know, those of us on the Gulf, most of us have very large ports in our area, and in particular the Port of Houston is one of the largest in the nation. So I would be interested in what the vulnerabilities would be on that.

I do want to acknowledge that for those of us who served on the Select Committee on Homeland Security, we have been working on this issue of port security for a very long time. I take note of the legislation by Loretta Sanchez and as well we offered a Democratic substitute, H.R. 1817. So we have been conversant with this, and then as a resident of Houston, we literally live by the port and understand some of its both deficiencies and its assets. When I say "deficiencies," not of the Port of Houston, but just by having a port.

I am reminded of after 9/11, if you will, the etching up of the Coast Guard, the U.S. Coast Guard that many have tended to take for granted, but have done an excellent job filling in for enhanced port security.

So having said that, I want to point out what seems to be driving us at this point, which is the Dubai Ports. I call it debacle and crisis without a negative alluding to Dubai in any way. But the incident was negative in terms of what it generated. The concern there was, of course, about who was in charge of security. There was seemingly some attempt to deflect that, oh no, Dubai Ports would not handle security. It is internally handled by the Coast Guard.

I think that is inaccurate because as a terminal operator, the terminal operator is by structure, as I understand it responsible for security. In this instance, Dubai Ports World would have been responsible for security of their terminals, and then the Coast Guard

would be the entity that checked for compliance with security plans.

From your knowledge, is that in fact true? And do you know how often the Coast Guard visits the terminal facilities to check compliance with security requirements? And does the Coast Guard engage in unannounced visits? I think that was a fine line on which we were raising our voices, that the intricate secrets of security at one port would certainly be similar to those in other ports, and you would be exposing the nation's ports to the possible review by individuals who would not have our best intentions.

If you would answer that, and let me just share another point with you that I would be interested in having you answer, is the House homeland security presidential directive which requires the development of a maritime infrastructure recovery plan to resume trade in the event of a terrorist act at a port. I would almost hope that they would amend that and include a natural disaster.

This plan has been delayed to incorporate lessons learned from Katrina, which is what I have just asked for. But as the plans have been delayed, my concern would be what vulnerabilities do we have as it relates to terrorist acts? When will the plan be completed? I would like to see a dual track. I would like to see us move forward on the existing response to terrorist acts, and work on the natural disaster, because we can be attacked at any moment. If the terrorist attack occurred at a port tomorrow, what would be the response?

I understand the Coast Guard would set maritime security conditions, but what would that mean for CBP? And couldn't the security actions required after an attack result in a shutdown even if a shutdown order is not given? I would appreciate your insight on those questions.

Chairman KING. Mr. Secretary, answer the questions here.

Mr. JACKSON. Okay. Yes, sir. Who is responsible for security? It is a shared responsibility under a government mandated regime that was established through MTSA and other authorities under law. The Coast Guard has this broad MTSA authority. Part of that requires terminal operating companies to have a certain security regime in place. So they have, as you asked me, affirmative obligations there.

The underlying regime in the security regime is that of the Coast Guard as established through law through MTSA. Similarly, the Customs and Border Protection has a security role in screening and inspecting cargo in a port facility. The port terminal operator does not know what container is going to be pulled, inspected or devanned. So this is a layer of protection about which specific containers we are worried about, and which specific actions will be mandated.

They sometimes have a role in helping us move a container from one place to the next, they oftentimes have that role, but it is at the direction of CBP that tells them and doesn't explain why that we want to look at a particular container. So the Coast Guard and CBP have therefore routine presence in the ports.

The Coast Guard's principal presence in the port is revolving around the captain of the port, a Coast Guard officer. In Houston, it is a senior Coast Guard officer that pulls together the port secu-

rity plan for the entire port and other port operational integration that is needed for the port. So the question about sharing the full security secrets of the U.S. government with a terminal operator is really not I think a particularly strong concern because most of the most precious and I would say confidential parts of this which relate to targeting are, again, not the terminal operators responsibility.

In the work that the Coast Guard does as a vessel approaches the terminal, in the work that we do to screen the vessel itself and the mariners on it, again a public function, not a private function. So it is a combination of responsibilities, all of which integrate into a layered system of security, but which is I think appropriately protected in terms of the confidentiality of the material.

On the second general question about maritime infrastructure recovery plan, that was part of the maritime domain awareness planning work that is required. We have a broad strategic plan that addresses this issue that has been published. We have a specific annex on this issue. This bill calls for further work on this question of recovery.

I think you are right to ask for us to focus carefully on recovery, not only from terrorist attacks, but natural disasters. When Hurricane Pam looked like it was headed up the Houston ship channel, I know that we spoke and we were all very concerned about the impact upon the economy in this vital national asset. So our contingency planning and re-starts should cover both of those threats.

Ms. JACKSON-LEE. Did you answer me to say there was a plan completed?

Chairman KING. The gentlelady's time has expired and we do have a second panel and we have run significantly over.

I want to thank the secretary for his testimony. We are awaiting the second panel. I would like to take the prerogative, though, of asking you a question which is going to be raised by each of the members of the second panel, I believe. I would just like to, if you could give us your statement on it so at least will have it in some context.

This is on CBP, with the ATS and the 24-hour notice. That, as I understand it, only requires manifest data. I think each of the witnesses are going to say that much more comprehensive cargo entry data would be required for that really to be effective. How would you address that so we will have this in context when each of the subsequent witnesses testify?

Mr. JACKSON. Mr. Chairman, I would agree that a richer set of data should be gathered to give us the next generation tools that we want in the targeting world, and that is core to the whole idea of secure freight, that we can gather, fuse and use the information about the pre-history of a given container that is more than just the weigh-bills information.

So I am in strong agreement with that, and that is a commitment of this department to get a richer data pool from which to do our screening.

Ms. JACKSON-LEE. Mr. Chairman, would you yield please? I want to make sure that Mr. Jackson is able to answer that question that I originally posed. I just wanted a simple yes or no as to whether

the plan is completed. If he could give that? The plan that had to do with the Hurricane Katrina impact is the original plan.

Mr. JACKSON. I understand that we have an annex on recovery that is completed. I will validate that and be happy to share that.

Ms. JACKSON-LEE. Would you please? I would greatly appreciate it.

Thank you, Mr. Chairman.

Chairman KING. Thank you.

I want to thank Secretary Jackson for his testimony. As always, we thank you for your cooperation. We look forward to working with you. I will take you up on the offer to—

Mr. JACKSON. I look forward to it. It will be a good day.

Chairman KING. Great. Thank you very much. The secretary is excused, and again I thank you very much for your testimony.

Mr. JACKSON. Yes, sir.

Chairman KING. Now, we will call the second panel. Let me thank each of the witnesses on the second panel for agreeing to testify today. I realize you had significantly short notice. I also know that each of you are very busy, so I want to thank you for taking the time to be here today, and also to thank you for the contributions that you have made to this whole issue of port security.

I will just briefly identify the witnesses. This is in no way giving them the accolades they deserve, but in the interests of time we will go through it quickly.

Mr. Christopher Koch, who is the president and CEO of the World Shipping Council; Mr. Jonathan Gold, who is vice president of Global Supply Chain Policy with the Retail Industry Leaders Association; Mr. Clark Kent Ervin, who is now a private citizen, but was the inspector general of the Department of Homeland Security; and Bethann Rooney, who is the manager of port security for the Port Authority of New York and New Jersey, and is involved not just in maritime security, but in air security as well.

In fact, it seems whenever I show up somewhere in New York to speak, she is there to make sure that the port authority doesn't get shortchanged. So even though you are hounding me and following me and harassing me, you are doing your job very well and I want to thank you for that.

I now recognize Mr. Koch.

STATEMENT OF MR. CHRISTOPHER L. KOCH, PRESIDENT AND CEO, WORLD SHIPPING COUNCIL

Mr. KOCH. Thank you, Mr. Chairman, and for the opportunity to be here today.

Our view of this is basically the strategy that DHS has established as a fundamentally sound strategy. For containerized cargo, they have a 24-hour rule strategy which means do your risk assessment before the container is loaded on the ship. We think that is the right strategy. The carriers which I represent provide the government with the data they have on those shipments 24 hours before loading. This is so-called the screening process.

The strategy then is to inspect 100 percent of the boxes that you have security questions about, and hopefully then get to the point of running through radiation scanners 100 percent of all containers coming into the United States.

And finally, the piece of build international agreements to extend this off our shores as best we can.

So if the strategy is sound, that doesn't mean there aren't opportunities for considerable improvements to how we implement those strategies. We thank the committee for trying to find those ways and work with the industry to get there.

A number of comments on H.R. 4954, which we have provided in more detail in our written comments, but a couple of points I would like to highlight. First is that we encourage the committee as they draft this bill to recognize that Congress already has passed a coherent framework for a lot of these issues. MTSA, the Marine Transportation Security Act, and the Trade Act, both passed in 2002, provide a fundamental strategy. We hope that in doing the amendments to the law that you will pass, that the layering of these new pieces come on top of it in a way that is not inconsistent.

Let me give an example. One of the priorities that we agree with this committee on is improving the trade data used for the targeting system. We think there is a consensus that needs to be done. The bill needs to be very clear, however, that it is consistent with existing law that says that data should be acquired before vessel loading, so that the targeting center in Northern Virginia can do the screening on that before it is put on the vessel. It doesn't do any good to get the data after it is already on the vessel. So there are some language changes we have identified in the bill already that we find very important and hope they are dealt with.

Secondly, we think getting the TWIC out is absolutely essential. It is already mandated by law. We recognize that, and it probably should not need another directive from Congress to mandate what has already been mandated, but if so, we are supportive of that. The bill before you right now does have a provision in it calling for an interim security screening of some sort of port workers. We are not entirely sure how that would work and we would like to discuss that with the committee after the hearing.

Finally, in terms of C–TPAT, the program is in place, as you know, by Customs. Some of the terms of the bill that try to mandate the provisions in C–TPAT we just urge the committee to consider carefully. Two in particular is whether or not you really want to hold importers accountable all the way back to the point of origin of where the goods are first manufactured and put in the smallest possible container. That is a kind of obligation that we think many importers would find very difficult to implement.

The second thing we would like to have you take a look at is the bill calls for container security devices to be put on boxes. For reasons we have outlined in some detail in our testimony, we have questions about whether or not that would be a realistic obligation for importers to be able to abide by.

The final two points I would like to make is we are, like Department of Homeland Security Deputy Secretary Jackson said, very interested and enthusiastic about the ICIS project. We think it has great potential, but there are a number of issues that would need to be worked out for it to become an operational reality.

So a final comment in relationship to the objective of that, which is to enhance the inspection of containers, we would note a number of concerns where the bill, H.R. 4899, the Sail Only If Scanned bill.

We do not think that is a realistic bill for reasons we have identified in our testimony. There are a lot of problems with it. We posed some questions to the committee of clarifications we think would be very important if that issue is going to become seriously discussed.

Thank you, Mr. Chairman.

[The statement of Mr. Koch follows:]

PREPARED STATEMENT OF CHRISTOPHER KOCH

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association representing international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93% of the United States' imports and exports transported by the international liner shipping industry, or more than $500 billion worth of American foreign commerce per year.[1]

I also serve as Chairman of the Department of Homeland Security's National Maritime Security Advisory Committee, as a member of the Departments of Homeland Security's and Treasury's Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Council. It is a pleasure to be here today.

In 2005, American businesses imported roughly 11 million loaded cargo containers into the United States. The liner shipping industry transports on average about $1.5 billion worth of containerized goods through U.S. ports each day. In 2006, at projected trade growth rates, the industry will handle roughly 12 million U.S. import container loads. And these trade growth trends are expected to continue. The demands on all parties in the transportation sector to handle these large cargo volumes efficiently is both a major challenge and very important to the American economy. At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to enhance maritime security, and do so in a way that does not unreasonably hamper commerce.

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

The DHS maritime security strategy involves many different, but complementary, pieces. It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and the Maritime Transportation Security Act (MTSA). It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code. It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one. The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area. And last, but certainly not least, these directives and efforts include an array of initiatives to enhance cargo security, including: (a) *cargo security* risk assessment screening, (b) the Container Security Initiative, (c) the Customs' Trade Partnership Against Terrorism (C–TPAT) Program, and (d) container inspection technology deployment.

I. *Introductory Comments on the Current Maritime Security Strategy*

[1] A list of the Council's members can be found on the Council's website at *www.worldshipping.org.*

The government's multi-layer security strategy is fundamentally sound, and seeks to address cargo and maritime security on an international basis as early as is practicable. It does not wait to address security questions for the first time when a ship and its cargo arrive at a U.S. port. Implementation of the strategy, however, can be further developed and strengthened.

It is very important to recognize that Congress has already enacted a broad, coherent statutory framework and set of authorities to address the maritime and cargo security challenge. The Maritime Transportation Security Act and the Trade Act, both enacted into law in 2002, address many of the issues under current discussion and in H.R. 4954 in a satisfactory manner. As a result, we recommend that new statutory provisions should be enacted when needed to fill specific gaps or to direct specific, needed actions. Care should be exercised not to add unnecessary layers of general statutory provisions on top of existing statutory authorities.

The maritime security challenge is to build on the fundamentally sound strategic framework that DHS has developed and to continue to make improvements on what has been started. Specifically, we believe that priority DHS consideration should be given to:

1. Improving the cargo shipment data collected and analyzed by Customs and Border Protection's (CBP) National Targeting Center before vessel loading. If cargo risk assessment is to be a cornerstone of DHS policy—which we believe is a correct approach, and cargo security screening is to be performed before the cargo is loaded onto a ship destined for the U.S.—which we also believe is a correct approach, it should be using more complete cargo shipment data to perform the risk assessment than only the ocean carriers' bills of lading;
2. Continue expanding international cooperation through the Container Security Initiative network;
3. Continuing to improve and strengthen the C–TPAT program;
4. Promulgating regulations to implement the MTSA mandate of maritime Transportation Worker Identification Cards for U.S. port workers; and
5. Undertaking a priority examination of the merits and feasibility of the Integrated Container Inspection System (ICIS) pilot project, the issues that would be involved in the widespread application of ICIS-type container inspection and radiation screening equipment, and the interface and use of such equipment and its results by Customs authorities.

II. *Foreign Investment in the Maritime Industry and Infrastructure*

Because the recent controversy in Congress over Dubai Ports World's acquisition of P&O Ports raised the issue of foreign investment in the maritime and port business, some comments on that issue are in order, particularly because there are bills introduced in the House to prevent foreign investment in the nation's maritime infrastructure.

Stevedoring and marine terminal operations are a service industry that is open to foreign investment. Billions of dollars of foreign investment has been made in the U.S. over recent years in this sector, and that investment has contributed substantially to a transportation infrastructure that is critical to moving America's commerce efficiently and reliably. The investment has come from Japanese, South Korean, Danish, British, Chinese, French, Taiwanese, and Singaporean businesses, just as American companies have been allowed to invest in marine terminal and stevedoring businesses in foreign countries.

The substantial majority of American containerized commerce is handled in U.S. ports by marine terminal operators that are subsidiaries or affiliates of foreign enterprises, usually the container shipping lines themselves. This is an international, highly competitive industry, providing hundreds of thousands of American jobs. The United States depends on it, and it in turn has served the needs of American commerce well, adding capacity and service as the needs of American exporters and importers have grown.

An important element of the U.S. government's position in international trade negotiations for many years, under both Democrat and Republican administrations, has been the importance of securing the ability of international investment to flow into various international service industries. It is a principle of substantial importance to many sectors of the American economy. There are many billions of dollars of American service industry investments around the world, including banking, insurance, food service, accounting, construction, energy, engineering, etc.

U.S. marine terminal facilities, whether operated by U.S. or non-U.S. owned companies, must and do comply with all the government's applicable security requirements. There is no evidence that terminal facilities' operations conducted by foreign controlled companies are any less secure, or in any way less compliant with security regulations, or in any way less cooperative with U.S. government security authori-

ties than U.S. controlled companies. In fact, these companies work closely and cooperatively with the Coast Guard, CBP, the U.S. military, and other U.S. law enforcement agencies.

This is an international industry and has been for many years. Less than 3% of American international maritime commerce is transported on U.S.-*flag* ships, and foreign owned carriers are responsible for the capital investment in most of those ships. American *owned* liner shipping companies transport roughly 5% of the trade, and their vessels are largely foreign flag.

The leading American liner shipping companies, such as Sea-Land, APL, and Lykes, were sold by their U.S. owners years ago to foreign companies, and neither the Executive Branch nor an informed Congress did anything to protest or stop this change. Foreign ownership of shipping companies and U.S. marine terminal operating companies has been part of our nation's economic make-up for years. We live in a global economy and society where it is simply a fact that most of this important component of the nation's "critical infrastructure"[2] is owned and operated by foreign companies. One might wish American companies were dominant industry actors, but they aren't. Further, U.S. financial markets have demonstrated little enthusiasm for international liner shipping due to its high capital investment requirements, cyclicality, and intense competition, as well as the fact that other nations' tax laws are more favorable to shipping.

The U.S. has been well served by the investment capital these foreign companies have made and continue to make in serving U.S. commerce.[3] The United States' economy and U.S. importers and exporters would be significantly harmed by policies that discourage or prevent this foreign investment. This is particularly true now with trade volumes pressing U.S. transportation infrastructure's capacity, and with ports, state governments, and the federal government all searching for additional investment capital to meet the nation's maritime transportation infrastructure needs and to keep American commerce competitive in the global market.

This nation is not at risk from foreign capital being invested in it, but it would be at risk if it were to discourage continued foreign investment in the maritime industry serving its needs.

There is another aspect to the recent Congressional interest in foreign ownership of marine terminal operators that has been myopic. In addition to the Dubai Ports World-P&O Ports transaction being mischaracterized as a purchase of U.S. ports—which it was not, and in addition to the fact that no facts were provided that showed DPW to be a security risk as a terminal operator—and in fact Dubai was shown to be an important ally and supporter of U.S. efforts in the Middle East and one which is trusted by the U.S. military to service its vessels and cargo. The entire controversy ignored the fact that, even with the six U.S. marine terminals being spun off from this purchase, DPW will be the third largest marine terminal operator in the world, and will be loading cargo onto vessels destined for the United States from its facilities in Australia, Europe, Asia and the Caribbean every day.

Wouldn't it make sense for the U.S. security strategy to try to include companies like DPW as partners of the government's efforts to secure international commerce? DPW is a knowledgeable and professional actor, both globally and in a particularly relevant part of the world. Instead, the Congress just told the third largest terminal operator in the world that it did not trust them, when the facts presented did not justify such a judgment of the company. The unfortunate treatment of this transaction should be kept confined to the narrowest possible application.

The international shipping industry and America's foreign commerce are global enterprises. Devising and implementing effective maritime security enhancements requires the participation and effort of many governments and many foreign owned and operated business enterprises. The U.S. government does not have the capa-

---

[2] The liner shipping industry and marine terminal operators logically fall within the most commonly used definitions of "critical infrastructure". *See, e.g.*, the National Infrastructure Protection Plan definition: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, networks or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The liner shipping industry transports roughly 11 million containers of imported goods per year to American importers and consumers, 7 million containers of exported goods from American businesses, and important government and military cargoes. The value of this goods movement is over $1.5 billion per day, and these supply chains connect the American economy to the rest of the world. The industry that is responsible for this transportation service is critical infrastructure.

[3] The hundreds of millions of dollars presently being invested in Portsmouth, Virginia by Maersk, in Mobile, Alabama by Maersk and CMA-CGM, and in Jacksonville, Florida by MOL are just three examples of this ongoing commitment to the construction of improved U.S. transportation infrastructure.

bility or the jurisdiction to do this by itself. It needs the cooperation and assistance of foreign governments and foreign owned businesses. The Coast Guard and Customs and Border Protection fully recognize this and are working to build and enhance global security strategies. Protectionism and unfounded criticism of foreign owned enterprises will impair those efforts and will impair security enhancement efforts.

III. *Comments on H.R. 4954, the SAFE Port Act*

We commend the Committee for its continued interest in maritime and cargo security, and for its interest in trying to fashion something that may be of constructive value out of the recent, unproductive controversy over the Dubai World Ports issue. We can provide the Committee staff with detailed section-by-section comments at a later time, and hope the following more general comments on the legislation will be helpful.

Section 4. Strategic Plan: It is appropriate for Congress to instruct DHS to develop a strategic plan for the security of the maritime transportation system, but it has already done so in MTSA (46 U.S.C. 70103). DHS has produced and continues to produce strategic plans for maritime security and infrastructure protection. Last fall, DHS issued its National Strategy for Maritime Security, and in addition is producing eight supporting strategic plans, including: the National Plan to Achieve Domain Awareness, the Global Maritime Intelligence Integration Plan, the Interim Maritime Operational Threat Response Plan, the International Outreach and Coordination Strategy, the Maritime Infrastructure Recovery Plan, the Maritime Transportation System Security Plan, the Maritime Commerce Security Plan, and the Domestic Outreach Plan. The Coast Guard also recently completed the Maritime Subsector plan component of the National Infrastructure Protection Plan.

There are plenty of strategic plans. We do not see a need for Section 4. Maritime security enhancements are more likely to come from implementing new security measures than instructing the bureaucracy to produce more strategic planning documents.

Section 5. Protocols for the Resumption of Trade: The Council supports this section's instruction that DHS develop protocols for the resumption of trade in the event of a transportation security incident, but notes that, based on our discussions with CBP and the Coast Guard on this issue, the issues involved are often highly dependent on the facts of the situation. One very important issue that should be made explicit, however, is that, once the federal government has issued its security approval for foreign or interstate commerce to move, state and local governments are preempted from second-guessing or trying to overrule or interfere with those federal decisions.

Section 6. Improvements to Automated Targeting System: This is perhaps the most important issue addressed by the bill. The existing and statutorily mandated strategy of the U.S. government is to conduct a security screening of all containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The correct time and place for the cargo security screening is before the containers are loaded on a ship.

In order to be able to perform this advance security screening, CBP implemented the "24 Hour Rule" in early 2003. Under this rule, carriers are required to provide CBP with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. CBP, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without further review. Every container shipment loaded on a vessel bound for the U.S. is screened through this system before vessel loading at the foreign port. Customs may issue the carrier a "Do Not Load" message on any container that is so screened if it has security concerns that need to be addressed.

The DHS strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100% of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100% of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5-6% of all inbound containers (roughly 600,000 containers per year), using either X-ray or gamma ray technology (or both) or by physical devanning of the cargo.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo

shipment have been addressed prior to a vessel being loaded. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy. Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to CBP for each shipment for the before-vessel-loading security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers's manifest data has limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities. *Currently, there is no data that is required to be filed into ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process.* This occurs, even though these parties possess shipment data that government officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port". Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until *after* the cargo shipment is in the United States, often at its inland destination—too late to be used for security screening purposes.

In September 2004, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide CBP with the following data elements before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check.), and
9. Origin of container shipment—the name and address of the business where the container was stuffed, which is often not available from an ocean carrier's bill of lading.

An ocean carrier's bill of lading by itself is not sufficient for cargo security screening. Risk assessment is being conducted on the basis of commercial documents that may not inform DHS of where the goods are actually coming from, who is buying the goods, who is selling the goods, or the name and address of the party that stuffed the container. It would seem logical that the earlier filing of these shipment data elements would improve CBP's cargo security screening capabilities.

The government needs to decide what additional advance cargo shipment information it needs to better perform pre-vessel loading cargo screening. It may include the data elements recommended above, or it may include additional desired data elements beyond that list. While this is not a simple task, it is important that progress be made on deciding what additional data should be obtained for this purpose, and it is important that the cargo interests, and not just carriers, be required to provide the relevant data in time to do the advance security screening before vessel loading in the foreign port.

The need to enhance the data used in the ATS has been recognized by DHS, by the Government Accountability Office, by CBP, by importers, and by carriers. It is important to note that MTSA has already established that the maritime cargo security screening system is governed by the "24 Hour Rule" strategy of "establishing standards and procedures for screening and evaluating cargo prior to loading in a foreign port for shipment to the United States." (46 U.S.C. 70116(b)(1)). Further, Section 343 of the Trade Act of 2002 *already* specifically authorizes and instructs DHS to establish mandatory advanced electronic information for cargo security screening, including the quite correct directive that "the requirement to provide particular information shall be imposed on the party most likely to have direct knowledge of that information".

What is needed is for DHS to develop and propose new regulations identifying and requiring the next generation of data for the ATS. While a new statute should not be necessary to achieve this, we support Section 6's effort to require such action, *but only if* its language is clarified that the additional cargo data is to be obtained *prior to vessel loading, not* "prior to importation". It is essential that this bill be consistent with the established before vessel loading security screening strategy of MTSA, as well as Section 343 of the Trade Act.

Section 7. Uniform Data for Government-Wide Usage We support this provision, and note that Congress has appropriated hundreds of millions of dollars on the

Automated Commercial Environment (ACE) system, which will hopefully meet this section's goals.

Section 8. Verification for Individuals With Access to Secure Areas of Seaports We fully support the Committee's efforts to expedite implementation of the MTSA requirements to establish a Transport Worker Identification Card (TWIC) program, although another statutory directive to DHS to implement the existing MTSA directive seems unnecessary. As to Section 8's "interim" initiative to have DHS compare transport workers with unescorted access to secure seaport facilities against terrorist watch lists, we are fully supportive in concept, but unclear how this process would actually work. We would welcome the opportunity to work with the Committee staff to better understand this.

Section 10. Container Security Standards and Verification Procedures Section 10 would require DHS to establish seal verification requirements within 180 days of enactment. This is an issue that is already addressed by MTSA (46 U.S.C. 70116). DHS and industry representatives have been working on it for some time. The challenges are several. First, it has become clear that without electronic seals and a global RFID e-seal reading infrastructure at ports around the world, such a requirement is not practical. Carriers themselves cannot verify seals before vessel loading; they will depend on foreign terminal operators at ports around the world to undertake such a task. It is for that reason that the Council and its member lines have been working hard to develop an international e-seal standard at the International Standards Organization. For many reasons, such a standard remains elusive. It is clear that implementation of such technology will take significantly more time. Second, an e-seal system and infrastructure would be very expensive, and security experts increasingly question whether such seals provide sufficient security benefits to justify the costs, particularly if more advanced, effective technology can be developed. Third, seal verification anomalies would be frequent, and both CBP and the industry have concerns that addressing the many thousands of expected anomalies, which are likely to have little national security implications, could be a difficult burden on the agency and commerce. Rather than adding another statutory layer on top of MTSA, we recommend the Committee obtain a full briefing on these issues from CBP and the industry. The information and issues involved are also relevant to Section 15 of the bill and its call for further research, development, testing and evaluation of technologies.

Section 11. Radiation Detection and Radiation Safety The Council supports this section, and would also observe that the DHS strategy on this issue should consider, not only the deployment of such radiation detection equipment at U.S. ports of entry, but how the "ICIS concept", with its possible deployment of such equipment overseas by marine terminal operating companies, may fit into the government's strategy. This topic is discussed in greater detail in the next section of our testimony.

Section 13. C–TPAT Like Section 12's treatment of CSI , it is appropriate to create a statutory foundation for this CBP program. We have several comments on this section. First, the Committee should carefully consider how far back in a supply chain it intends to hold a C–TPAT importer accountable. The bill's definition of "point of origin", going back to the point where goods are assembled into the "smallest exterior packaging unit", may be feasible for some importers that order directly from a foreign manufacturer, but would probably be impossible for importers of many commodities and traded goods, and could be impossible for large importers that use many suppliers.

Second, we note that in proscribing the Tier Three program for C–TPAT importers, the bill would encourage "container security devices" (CSDs). We believe CSDs are not yet appropriate for inclusion in the program for the following reasons: (1) Neither the bill, DHS or the trade have developed clear definitions of what the requirements for such devices should be. Depending on who you talk to, it might include seals, electronic seals, the CSDs that were recently tested by CBP in its pilot tests, or "Advanced CSDs" being tested by Science and Technology within DHS. Do they have to have sensors that detect intrusion into the container via one door, via either door, through the walls? Do they have to detect conditions other than intrusion? (2) The possible technologies vary from using RFID (although there is not agreement on what radio frequency should be used for RFID) to wireless/satellite devices. (3) To be effective and deployed on a commercial basis, RFID CSDs would require a global reading infrastructure to be built at ports around the world. That infrastructure does not presently exist. (4) There is no agreement on who would operate and control the CSD reading infrastructure or the information generated if RFID technology is used. (5) There is no agreement on how a marine terminal would know that a container arriving into it was supposed to have a CSD on it to be read. (6) There is no protocol in place for how to address anomaly readings or

alerts that would be generated from CSDs. (7) There is no international standard for CSDs, and an internationally usable and accepted standard would be essential. The Council has been working diligently for several years at the International Standards Organization on the effort to establish a standard for electronic seals, and we have not yet succeeded. The process for establishing such a standard for CSDs has not even begun. (8) Many CSDs being discussed have the ability for persons to change or write new information into them after the container is closed. The security questions arising from the ability to write new information into such devices have not been resolved. (9) Acceptable error rates have not been satisfactorily established.

CSDs have a potentially important role for future container security enhancement, but they are not yet ready for inclusion as an element of the Tier Three importer concept.

IV. *Comments on H.R. 4899, the "Sail Only if Scanned Act of 2006"*

While this hearing is on H.R.4954, H.R. 4899 was offered as an amendment to this bill in Subcommittee and defeated. Because it appears possible that H.R. 4899 will be offered again as an amendment to H.R. 4954, and because it was defeated by only an 8–6 vote, some comments on this bill are offered for the Committee's consideration.

We respectfully submit that H.R. 4899 is poorly drafted and raises many unanswered questions. Even more importantly, if it were actually enacted into law and implemented, it would have a devastating impact on American commerce and the American economy. Some comments and questions on this bill follow.

First, the stated intent of this bill is to require every container of cargo to be scanned before being loaded onto a vessel bound for the U.S., and further that, if the container has not been scanned in the foreign port of loading in accordance with the terms of bill, it cannot be loaded aboard a vessel bound for the U.S. (ergo, the "Sail Only if Scanned Act") This would be impossible to implement, at least in the time frame and under the terms of this bill, because the equipment, systems, operating protocols, and necessary international agreements are not in place. If H.R. 4899 were enacted into law and enforced, it would bring America's containerized foreign trade to a halt.

Second, the bill requires that each container be *"scanned"* with equipment that meets certain standards, but it does not make it clear what *"scan" means. Does it mean radiation scanning, or does it also* mean gamma ray or X-ray non-intrusive inspection image scanning (NII)? Obviously, it is important to be clear about what is being required. These are two different technologies and processes.

Third, the bill requires that each container be scanned and that a copy of the scan be provided to the Secretary, but it does not say *who* is to do the scanning. We believe the bill's authors should clarify whether the bill is proposing that the scan be done by the marine terminal operator that is loading the vessel, or whether the scanning must be performed by foreign governmental authorities at the particular port of loading. As the bill provides no funding for the implementation of this overseas container scanning requirement, we presume that the authors intend the cost of equipment acquisition and system operation will be borne by whomever they identify as the parties who are expected to perform the scanning task. Clarity on this point is very important.

Fourth, the bill states containers must be scanned before they are loaded onto vessels bound for the U.S., and a copies of the scans must be sent to DHS, but it fails to say *when* the scans must be sent to DHS, *how* they would be sent, or *what* DHS is expected to do with them when it receives them and within what time frame. A scan that is not analyzed or acted on is without value.

Fifth, the bill would require DHS to establish scanning equipment technology standards, and then require that every major foreign government or marine terminal operator in the world adopt that standard, buy, install and operate that equipment, and apply it to all of their exports to the U.S. within 12 months.

Sixth, we don't yet have a technology standard for RFID electronic seals, yet the bill proposes changing the emerging e-seal technology from RFID to satellite technology.

Seventh, if the bill became law, it would almost certainly invite other countries to establish reciprocal requirements for U.S. exports, so that U.S. goods could not be exported, unless the U.S. government or U.S terminal operators had scanned the container before vessel loading in a U.S. port, used technology that met a foreign government's standards, and sent the scan to the foreign government. The bill's proponents may wish to consider how would they would feel if the Chinese or Japanese or British governments said there can be no U.S. exports to their country unless the U.S. installs and operates container inspection equipment, which meets Chinese

or Japanese or British government technology standards, and sends the scan images to their government.

Finally, we have tried to consider the cost of this requirement, but it is difficult to assess the cost of complying when it is not clear if the "scan" is intended to require radiation scanning or both radiation scanning and NII imaging analysis, and when the necessary equipment and systems simply are not in place to perform the task. Someday in the future, if the "ICIS concept" is validated and implemented, there may be systems in place to provide advance, pre-vessel loading screening for a large percentage of American containerized commerce, but it would be very difficult to ever reach 100%. At present the systems simply are not in place to do this. To estimate costs, one might consider that the average cost of an NII container inspection in a U.S. port seems to range from $100 to $125 per container, with a 1–3 day delay in releasing the cargo. The more containers inspected, the higher the congestion, terminal, personnel, and operating costs. A linear projection of $125 per container to 11 million import containers would exceed $1.3 billion, but that projection would not even begin to consider the "chaos" costs that would ensue in port facilities trying to perform such a task, nor would it consider the costs of the likely application of this requirement to U.S. export containers, nor would it consider the enormous costs of the delayed delivery or non-delivery of commerce. Suffice it to say that compliance and consequential costs of the bill would be staggering.

Container inspection technologies, including non-intrusive inspection (NII) equipment and radiation screening equipment, clearly have an essential and growing role in increasing both the efficiency of inspecting containerized cargo shipments and the number of containers that can be inspected. Container inspection technology, particularly NII equipment, is of substantial interest because, unlike so many other technologies, it helps address the container security question of paramount importance, namely: "What's in the box?"

The Committee's limitation on the length of testimony does not allow a fuller description of these issues in this forum, but the Committee is invited to review the Council's March 30th testimony before the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs for a fuller discussion of these important issues, including a discussion of the Hong Kong pilot project called the Integrated Container Inspection System or "ICIS concept".[4]

We thank the Committee for the opportunity to present these views.

Chairman KING. Mr. Koch, thank you for the conciseness of your testimony.

I will just remind the other witnesses that the full statements will be inserted and made part of the record.

The chair now recognizes Mr. Jonathan Gold. Mr. Gold?

STATEMENT OF JONATHAN GOLD, VICE PRESIDENT, GLOBAL SUPPLY CHAIN POLICY, RETAIL INDUSTRY LEADERS ASSOCIATION

Mr. GOLD. Thank you, Mr. Chairman, for the opportunity to testify today on this important issue. We, as members, share this committee's goal of making the movement of cargo to the supply chain as safe and as secure as possible. As some of the largest users of the system, we have an enormous stake in supply chain security and are committed to helping the government further enhance security throughout the system.

While a great deal has been accomplished to improve supply chain security since the tragic events of September 11, the government and private sector stakeholders must continue to work together to improve security.

We strongly believe that the U.S. can achieve the dual objectives of enhanced security and facilitation of legitimate global commerce. We urge Congress to avoid measures that have a very limited effect

[4] That testimony is available on the WSC website at *www.worldshipping.org*

on enhancing security while actually impeding the flow of legitimate commerce in creating a false sense of security.

Supply chain security is a global issue that cannot be addressed unilaterally. The most effective supply chain security measures are those that push our borders out, assessing vulnerabilities and identifying threats to cargo shipments before they reach U.S. ports. Effective supply chain security requires a multilayered, unified approach that must be international in scope.

Let me move on to some comments on the bill itself. RILA strongly supports the development of a strategic plan for supply chain security. We believe that the initial version as planned already exists under the National Strategy of Maritime Security. Further efforts should improve this plan; in particular, the Maritime Incident Response Plan.

RILA commends the committee for supporting confident planning and restoration of trade in the event of a maritime security incident.

The United States is in dire need of a well-coordinated response plan to ensure that commerce continues to move throughout the supply chain should an incident occur.

In addition, Congress and the administration need to ensure that the various agencies involved in Homeland Security do not duplicate ongoing efforts.

While security concerns may require that certain details need to be kept within the government's sphere, RILA believes that a central communication point or channel must be established so that communications can be streamlined.

One need to only look at the experience of Hurricane Katrina to understand the need to have a well-coordinated response.

CBP receives detailed information about every container coming into the U.S. prior to that container being loaded at a foreign port to differentiate the true needle in the hay stack to the overwhelming percentage of cargo containers that present no security risk. Setting arbitrary and mandatory percentages of cargo that must be physically inspected would do nothing to enhance security and would actually undermine it.

Better identification of high-risk cargo represents the best use of government resources that should be the goal of this and any legislation addressing cargo security.

RILA is committed to improving container screening by identifying additional cargo data that can help with the identification of high-risk cargo.

In keeping with increasing security at U.S. ports, RILA also endorses the prompt implementation of the Transportation Workers Identification Credential.

Security must be built into the global supply chain from origin to delivery, leveraging the best of current and emerging technologies. Put simply, there is no technological silver bullet for supply chain security. We must be wary of adopting technological solutions that merely create a false sense of security. Too much is at stake to put our trust behind cosmetic feel-good security measures.

It is important that promising technologies be developed by dedicating adequate funds for research and development. Congress should outline policies and goals and allow industry to work with

DHS to find the smartest and most effective way to meet those goals rather than being forced in deploying unproven gadgets.

RILA supports efforts to ensure that we have a zero-tolerance policy for nuclear and radiological materials entering our country.

While it is preferable to have the screening done overseas, we will need to have a robust detection regime at our domestic ports as well.

In addition to the deployment of the radiation portal monitors at U.S. ports, RILA also encourages DHS and CBP to consider other models to help conduct container screening overseas. One such model which has received a great deal of attention is the ICIS system, which is currently being tested at two terminals in Hong Kong.

While we, along with CBP, believe that this model fits with the multilayered approach, a number of issues must be resolved before such a system is implemented on a global scale.

The key to C–TPAT's success is—acknowledgement that there is no one-size-fits-all approach to supply chain security. What works for one industry, such as retail, may not be well-suited for another industry such as chemical.

RILA opposes any proposal that will limit the ability of government and industry to respond to and adapt quickly to innovations and other changes related to the security dynamics of their specific link in the supply chain.

We are also concerned that the public-private partnership concept at the heart of C–TPAT's effectiveness would by compromised by the introduction of required third-party validators.

C–TPAT works because it provides incentives to participants to engage in active compliance with government security objectives.

While the focus on today's hearing is on the SAFE Port Act, I would be remiss in not commenting about the Sail Only if Screened Act of 2006, which was offered as an amendment during last week's markup.

RILA supports 100 percent screening of high-risk containers, but a policy requirement of 100 percent scanning of all U.S.-bound containers is neither effective as a deterrent nor feasible operationally.

Rather than enhancing security sending an arbitrary number of scanning or inspections of the containers will create much of the same harm to the nations and world economy that a terrorist incident would cause.

While the bill calls for scanning of all containers for radiation and density, again, as Chris has pointed out, these terms are very vague. There are also many questions about who will be conducting the scanning, when the scanning would occur, to whom the scanned images will be sent, and what would be done with the images once they are received.

The bill also includes requirements for a container seal that can detect and track whether a container has been tampered with after loading. We fully believe the technology to accomplish this goal is still being tested and should not be mandated at this point in time.

I thank the committee for the opportunity to testify today and welcome any questions.

[The statement of Mr. Gold follows:]

PREPARED STATEMENT OF JONATHAN GOLD

Good morning. Chairman King, Ranking member Thompson and other distinguished members of the committee. My name is Jonathan Gold and on behalf of the Retail Industry Leaders Association (RILA), I thank you for the opportunity to testify at this important hearing regarding the Security and Accountability For Every (SAFE) Port Act.

By way of background, the Retail Industry Leaders Association (RILA) is a trade association of the largest and fastest growing companies in the retail industry. Its member companies include more than 400 retailers, product manufacturers, and service suppliers, which together account for more than $1.4 trillion in annual sales. RILA members operate more than 100,000 stores, manufacturing facilities and distribution centers, have facilities in all 50 states, and provide millions of jobs domestically and worldwide.

I also serve as a member of the Department of Homeland Security's Advisory Committee on the Commercial Operations of Customs and Border Protection (COAC). Prior to serving on the COAC I participated in several of the subcommittees as a technical advisor, including the subcommittee working on implementation of the 24-Hour rule, implementation of the Maritime Transportation Security Act and the Customs-Trade Partnership Against Terrorism (C–TPAT) subcommittee, which helped to update the importer criteria last year.

RILA members share this Committee's, and indeed all Americans, common goal of making the global supply chain and the movement of cargo through the global supply chain as safe and secure as possible. As the largest users in the global maritime supply chain, we have an enormous stake in cargo security and are committed to helping the government further enhance security throughout the system. While a great deal has been accomplished to improve supply chain security since the tragic events of September 11, 2001, the government and private sector stakeholders must continue to work together to improve security. RILA commends the members of this Committee for striving to identify and address the vulnerabilities in our maritime supply chain system.

We strongly believe that security legislation, regulations, and public-private partnerships can achieve the dual objectives of enhancing security while continuing to facilitate legitimate global commerce. We urge Congress to avoid measures that have a very limited effect on enhancing security while actually impeding the flow of legitimate commerce and creating a false sense of security. A primary goal of those who would disrupt the supply chain is to damage the U.S. economy by any means possible. If commerce is disrupted in a way that damages the ability of Americans to hold well-paying jobs, provide for their families, and generate economic growth that helps the entire world, either through an attack or ill-conceived regulation of our international trading system, then the terrorists will have achieved one of their key goals.

Supply chain security is a global issue that cannot be addressed unilaterally. The most effective supply chain security measures are those that push our borders out, assessing vulnerabilities and identifying threats to cargo shipments before they reach U.S. ports. Effective cargo security requires a multi-layered, unified approach that must be international in scope. While recent policy debates have focused on who owns assets in the supply chain system, nobody should dispute that it is better to detect or disarm weapons or contraband thousands of miles from our shores than after their arrival in the U.S.

RILA and its members have played a critical leadership role in shaping supply chain security efforts. From requiring new security language in contracts with their business partners to testing new technologies and ways to identify container tampering, private sector stakeholders have been the innovators in securing their supply chains to protect their employees, customers and businesses. In considering the SAFE Ports Act, we urge Congress to continue to allow the private sector, working closely with the Department of Homeland Security and other government and non-government interests, to test and deploy the systems and technologies that prove most effective. No one has a greater interest in security than the private sector companies who depend on a secure and efficient supply chain for the safety of their employees and customers and efficient operations of their businesses.

As members of the Committee are aware, a number of regulations and initiatives have already been undertaken to protect the U.S. from a terrorist attack affecting the supply chain. RILA members have supported a number of these initiatives, such as the Customs-Trade Partnership Against Terrorism (C–TPAT), the Container Security Initiative (CSI), the 24-Hour Rule, the Bioterrorism Act, the Maritime Transportation Security Act (MTSA) and the International Ship and Port Facility Security Code (ISPS). Targeting different aspects of supply chain security, these regulations

and initiatives together represent a strong foundation upon which the SAFE Ports Act and other initiatives must build to enhance our nation's maritime supply chain security.

On March 9, RILA wrote a letter to every member of Congress suggesting some key areas where both Congress and the Department should focus on to improve cargo security. These include:

- Improve the Automated Targeting System to ensure Customs and Border Protection (CBP) has the right information to determine whether or not a container poses a risk.
- Ensure CBP has sufficient resources to conduct C-TPAT validations.
- Work with CBP to improve CSI to conduct more cargo screening abroad, with a special emphasis on the quality of screening for nuclear and radiological material.
- Ensure that all aspects of MTSA are implemented, including the Transportation Worker Identification Credential (TWIC).
- Further develop business continuation and restoration of trade plans.

In most respects, the SAFE Ports Act is well aligned with these recommendations. For purposes if this written testimony, I would like to discuss some of the key sections of the bill and share RILA's perspective:

Section 4—Strategic Plan

RILA strongly supports the development of a strategic plan for cargo security. We believe that an initial version of this plan already exists under the National Strategy on Maritime Security. Further efforts should seek to improve this plan and its eight supporting plans, in particular the Maritime Incident Response Plan.

Section 5 Protocols for the Resumption of Trade

RILA members commend the Committee for including consideration of mechanisms to provide for continuity planning and restoration of trade in the event of a maritime security incident. The United States is in dire need of a well-coordinated response plan among all levels of government to ensure that commerce continues to move throughout the supply chain should an incident occur. In addition, Congress and the Administration need to ensure that the various agencies involved in homeland security do not duplicate ongoing efforts. In short, the government, the business community and key stakeholders throughout the international trading system must be on the same page and know there is a plan in place to respond to an incident of national significance occurring as a result of terrorism or national disaster.

For example, if an incident were to occur in the Port of Los Angeles, that port, as well as the Port of Long Beach, might have to be shut down during the incident investigation and response. What would happen to other ports on the West Coast? Would Seattle/Tacoma remain open? Would incoming cargo be able to be diverted to other ports? While individual ports have worked on contingency plans for their own facilities, have there been discussions among ports geographically located near each other as to how they would work together? Will all maritime vessels be required to stop where they are or will vessels at non-incident ports be allowed to continue to move?

It is not clear to the business community at this time as to who will be making these critical decisions. The trade community needs this vital information to plan appropriately. While security concerns may require that certain details need to be kept within the government sphere, RILA believes that a central communication point or channel must be established so that communications can be streamlined. DHS has begun to work on this issue with the release of the Maritime Incident Response Plan, but more work needs to be done. One needs only to look at the experience of Hurricane Katrina to understand the need to have a well-coordinated response that ensures commerce will continue to flow through our nations' ports in the wake of an incident.

Likewise, each country has an interest in ensuring that the global supply chain is kept safe. A major terrorist incident in the U.S. will not impact just one port or one city or even one country. The impact will be felt around the globe. Careful planning and cooperation among governments is important, and government's active collaboration with the private sector is extremely critical. Supply chain security is simply too complicated for the public sector to act effectively without partnering with private industry.

Section 6—Enhanced High-Risk Targeting Capabilities

CBP receives detailed information about every single container coming into the U.S. prior to that container being loaded at a foreign port, and has developed elaborate mechanisms to utilize intelligence and other risk factors to differentiate the true "needle in the haystack" from the overwhelming percentage of cargo containers

that present no security risk. Again, setting arbitrary and mandatory percentages of cargo that must be physically inspected will do nothing to enhance security and would be contrary to the mission of the effective risk management system DHS already has in place.

Better identification of high-risk cargo represents the best use of government resources and should be the goal of this and any legislation addressing cargo container security. RILA is committed to improving cargo container screening by identifying additional cargo data that can help with the identification of high-risk cargo. DHS should work with cargo owners and others who own supply chain information to determine what data elements are needed for security risk assessment, who has the information, when the information can be submitted, how it will be used and, most importantly, how it will be protected.

Section 8—Verification of Individuals with Access to Secure Areas of Seaports

In keeping with increasing security at U.S. ports, RILA also endorses prompt implementation of the Transportation Workers Identification Credential (TWIC), a standardized ID containing biometric information that vets the identity and background of the cardholder. All individuals with access to cargo and secure areas of our nation's ports would carry the TWIC, and its potential for use extends to workers throughout our nation's critical infrastructure systems. We believe that verification of individuals with access to secure areas of critical infrastructure and identification of individuals with prior criminal records or indications of connections with terrorist elements are crucial steps toward strengthening security.

Section 10—Container Security Standards and Verification

Security must be built into the global supply chain from origin to delivery, leveraging the best of current and emerging technologies. Yet the recent GAO report also underscores the need to keep in mind that technology is only one part of the overall solution. Put simply, there is no technological "silver bullet" for supply chain security. We must be wary of adopting technological solutions that merely create a false sense of security. Too much is at stake to put our trust behind cosmetic, "feel good" security measures.

RILA encourages appropriate testing of all proposed technology solutions to determine which have the greatest reliability before being adopted by the government and industry. It is important that promising technologies be developed by dedicating adequate funds for research and development. At the same time, rushing unproven and/or faulty technology into supply chain security without thorough implementation testing solely for the sake of doing something about security will undermine progress made to date, contribute to a false sense of security and in the end, prove both costly and ineffective. The fact that a certain physical device or screening process may work well in a lab or at a particular port does not mean that it can or should be expanded to other real-world applications. Congress should outline policies and goals and let DHS find the smartest and most effective way to meet those goals rather than being forced into deploying unproven "gadgets." Before any technology can be mandated, DHS must ensure the technology's functionality and application as well as work with the trade community to determine the most effective methods to deploy them in order to achieve maximum results.

Section 11—Nuclear and Radiological Detection Systems

As DHS works to improve its supply chain security capabilities, RILA supports efforts to ensure that we have a "zero tolerance" policy for nuclear and radiological material entering our country. While it is preferable to have that screening done overseas as occurs at CSI ports covering the great majority of cargo bound for the U.S., so long as we allow smaller ports to ship to the U.S., we will need a robust detection regime at our domestic ports as well. Thus it should be the highest priority for CBP and DHS to ensure that those ports participating in the Container Security Initiative have the most effective technology available to detect radiation and that domestic ports achieve universal nuclear and radiological detection capability. Recent Government Accountability Office reports have identified weaknesses in both aspects of the nuclear and radiological detection regime, and RILA supports the work of the Domestic Nuclear Detection Office to build this most critical layer of our defenses.

In addition to the deployment of the Radiation Portal Monitors at U.S. ports, RILA also encourages DHS and CBP to consider other models to help conduct container screening overseas. One such model, which has received a great deal of attention, is the Integrated Container Inspection System (ICIS), which is currently being tested at two terminals in Hong Kong. While we, along with CBP, believe that this model fits with the multi-layered approach, there are still many questions and oper-

ational issues that need to be discussed and resolved before such a system is implemented on a global scale. We strongly urge DHS and CBP to continue to work with the private sector on ICIS and other models to successfully address the operational issues.

Section 13—Customs-Trade Partnership Against Terrorism

One cornerstone of the public-private, collaborative approach to supply chain security supported by RILA is the C–TPAT program, which reflects CBP's recognition that it can best provide security through close cooperation with the very businesses whose ability to recognize potential vulnerabilities in the supply chain is matched only by their desire to ensure that the system as a whole—and each component part—is as robust and secure as possible. The key to C–TPAT's success is the program's acknowledgement that there is no "one size fits all" approach to supply chain security, for individual C–TPAT member's supply chain functions, needs and vulnerabilities are not the same. What works for one industry, such as retail, may not be well suited for another industry, such as chemical.

While there has been some consideration given to placing C–TPAT under a strict regulatory regime, RILA members strongly believe that regulating this program will limit the very flexibility that is one of the program's greatest assets, and in turn harm the ability of government and industry to respond and adapt quickly to innovations and other changes related to the security dynamics of their specific link in the supply chain. Requiring changes to C–TPAT to go through a full regulatory rulemaking process would be much slower and less nimble for CBP to turn current intelligence or perceived weaknesses into new security requirements.

In addition, the public-private partnership concept at the heart of C–TPAT's effectiveness would be compromised by the introduction of required "third party validators" acting as middlemen between government and the business community, adding a potentially cumbersome extra layer of communication to a direct, two-party dialogue. With a third party attempting to interpret and relay information from business to government, the potential for diminishing and delaying the quality of information exchanged is clear.

C–TPAT works because it provides incentives to participants to engage in active compliance with government security objectives by, for example, providing ATS scoring benefits to companies that meet the basic requirements of the program. RILA believes that continuing effective operation of the program depends on its ability to offer such baseline incentives for participation.

In addition, while we agree with the tiered approach as outlined by the bill and which CBP is currently using, we have concerns with Congress specifying what criteria companies must meet to achieve Tier Three status, especially the inclusion of language on container security devices. We do not believe Congress should mandate such devices as they are still being tested and are not yet at 100% overall reliability and still have many operations questions that need to be answered.

"Sail Only if Scanned Act of 2006" Comments

While the focus of this hearing is on the SAFE Ports Act, I would be remiss in not making some comments about the "Sail Only if Scanned Act of 2006," which was offered as an amendment during last week's markup.

RILA supports 100% *screening* of high risk containers, but a policy requiring 100% scanning of all U.S. bound containers is neither effective as a deterrent nor feasible operationally as a security enhancement measure. Rather than enhancing security, setting an arbitrary number of scanning or inspections of containers would result in commerce grinding to a halt, in effect creating much of the same harm to the nations and the world's economy that a terrorist incident would cause.

The legislation as drafted is very vague and confusing. While the bill calls for "scanning" of all containers for radiation and density, this term is not specifically defined. Is this a scan for radiological material? Is it a scan using a non-intrusive X-ray? These are two very different technologies that have different requirements and have different impacts on the movement of legitimate cargo.

There are also many questions about who would be conducting the scanning when the scanning would occur, to whom the scanned images would be sent and what would be done with the images. There is also a question whether the U.S. can mandate such a requirement on foreign terminal operators and foreign governments, which is why CBP has negotiated cooperative agreements, such as the Container Security Initiative, with foreign countries to allow screening on their soil. In addition, if we ask our foreign trading partners to put such a requirement in place, we must be prepared to do the same here in the U.S. as calls for reciprocity will surely be made.

In addition, the bill includes requirements for a container seal that can detect and track whether a container has been tampered with after loading. As discussed

above, technology to accomplish this goal is still being tested in the harsh real-world environment in which international cargo must exist.

Conclusion

I would like to thank the House Committee on Homeland Security for the opportunity to testify today. RILA applauds the initiative of the Committee to further enhance supply chain security and congratulates Chairman King, Chairman Lungren, Ranking Members Thompson and Sanchez and Congresswoman Harman and their staffs for focusing attention on these key issues. RILA strongly believes that government, industry and other stakeholders need to maintain an ongoing, robust dialogue on how best to strengthen port and supply chain security, rather than allowing the debate to intensify and recede as dictated by external factors.

RILA and its members stand ready to continue to work with both Congress and the Administration on improving the security of U.S. ports and the global supply chain. I look forward to taking your questions.

Chairman KING. Thank you, Mr. Gold.

Mr. Ervin?

STATEMENT OF CLARK KENT ERVIN, PRIVATE CITIZEN, FORMER INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

Mr. ERVIN. Thank you very much, Mr. Chairman. If time permits, I will talk about the other parts of my prepared remarks where I talk about the vulnerabilities and C–TPAT, the fact that we have too little radiation detection equipment, and the vulnerabilities in the equipment that we have, and then my comments about the bill itself. But I would like to confine myself largely to comments about the distinction between inspection and screening, because I think it is tremendously important.

There are two key statements here. One is that 100 percent of cargo is screened, and the other is that 100 percent of all high-risk cargo is inspected. Seems to me that the first statement is not only wrong, it is also misleading. And the second statement is wrong. Let me explain.

I wonder why the term "screening" is used at all, because as a number of members suggested, the average person infers, when he or she hears the term "screen," that that means inspected. We know that that is not the case, but the average American does not. Not only is it misleading, it is also erroneous as was pointed out by one of the members, a recent GAO report. It was just last year. I think it was in the fall of last year. The meeting was only a few months ago.

Our own congressional investigators said that 35 percent of cargo is not screened, not targeted, not profiled, whatever word you want to use, not assessed to determine whether it is high risk or low risk. So that means that the universe, the cargo that is being evaluated by CBP, is only two-thirds of the cargo that comes into our country. One-third of cargo that comes into our country we know nothing about. For all we know, some of that cargo could well be high risk, and the probabilities are that some of it is.

With regard to the two-thirds that is assessed, a GAO report from just last week on top of—I am sorry, it was a report of the Senate Governmental Homeland Security Committee—in addition to GAO reports and inspector general reports, which I presided over when I was the inspector general, have all pointed out flaws in the system upon which the targeting process is based, the ATS system. Because it is flawed, we don't know for sure whether we

are making adequate assessments of whether a cargo container is high risk or low risk.

With regard to that that we do determine for whatever reason is high risk, the report of the Senate committee just last week pointed out, as we have discussed here, that 17.5 percent of the time, almost a fifth of the time, foreign inspectors in this CSI program refused to inspect cargo that we deemed to be high risk.

Now, Secretary Jackson said, well, there is a difference between referrals and requests, and indeed there is. But the Senate report did not say, we have asked those countries to make a determination. They made that determination. That determination satisfied us.

Instead, what the report says is, we requested that an inspection be done, and the inspection was not done. Indeed, in France, about 60 percent of the time, according to this report, when we asked that an inspection be done, the inspection was not done.

My question is: Why do we have a program like this where foreign countries are asked to inspect things and they are not, in fact, inspected? The whole theory behind it is that the borders should be pushed out, as indeed they should be, because it might well be too late when a cargo container comes into the United States.

Furthermore, we are told that we should worry about that because in those instances where foreign countries refuse to inspect cargo that we deem to be high risk and that we say should be inspected, it is inspected here. A GAO report from last year said that at least 7 percent of the time that high-risk cargo is not inspected here in the United States as well.

So these are hugely important issues. What needs to happen is the Hong Kong system that we have been talking about here today needs to be implemented in the United States. I have not heard a single detail about exactly what practical limitations there are that prevent the implementation of that system here in the United States.

As was pointed out, exactly the same argument was made before 9/11 about the impracticalities and about the impacts economically of 100 percent of inspection of passenger baggage, and yet, of course, we do that today.

And furthermore, the secretary has said that the goal is to have 100 percent of inspections of cargo once it arrives in the United States and before it is dispersed to the rest of the country. It is unclear to me why there is a disconnect between the goal there and the goal with regard to cargo that comes into the country. Failing that, though, we at least need to have a better ATS targeting system so, in fact, we do target or screen 100 percent of cargo and so that, in fact, the 100 percent of cargo that we deem to be high risk based upon a better ATS system is, in fact, inspected. Neither of those things happens now today. At a minimum, they should, in my judgment.

Thank you very much.

[The statement of Mr. Ervin follows:]

PREPARED STATEMENT OF CLARK KENT ERVIN

Thank you, Chairman King, and Ranking Member Thompson, for inviting me to testify this afternoon on a bill, H.R. 4954 (the "Safe Port Act"), designed to enhance maritime and cargo security. This could not be a more timely and important topic.

If there is any good news to emerge from the recently scuttled proposed sale of terminal operations at six American seaports to a Dubai-owned company other than the fact that the deal was scuttled, it is that it has highlighted just how vulnerable our ports already are to terrorist penetration.

Thanks to the debate over the Dubai deal, more Americans have come to learn that only about 6% of the 27,000 or so containers that enter our seaports each day are inspected to determine whether they contain weapons of mass destruction or other deadly cargo, including terrorists themselves. The Department of Homeland Security has consistently claimed that we should not be troubled by this low percentage because the Customs and Border Protection's "targeting" efforts are so precise that we can be assured that the 94% of cargo that is not inspected is low-risk. However, studies by the DHS Office of Inspector General, the Government Accountability Office, and, just last week by the Senate Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations have all found the "ATS" (for, "Automated Targeting System") used by Customs to distinguish between high and low-risk shipments to be flawed.

The other program that Customs cites to comfort those who rightly believe that a 6% inspection rate is far too low is the "Container Security Initiative," or "CSI." The theory behind CSI is unassailable—if a container with a weapon of mass destruction inside is not inspected until it arrives at an American seaport, it might be too late. So, through CSI, Customs "pushes the border out," by obtaining the agreement of foreign ports to inspect containers bound for the U.S. before the ships that carry them set sail.

The problem, though, is that foreign inspectors often refuse to inspect containers that we Americans deem to be high-risk. Less than a fifth of the containers that we believe should be inspected abroad—17.5% to be precise—are in fact inspected by foreign ports. Ports in France, for example, refuse to inspect about 60% of cargo we deem to be high-risk. Furthermore, because, as noted above, the ATS targeting systems is flawed, chances are we should be requesting more inspections than the 13% worldwide that we are requesting.

Another program that Customs disingenuously touts as a cargo security measure is the CTPAT or Customs Trade Partnership Against Terrorist program. Companies in the global maritime supply chain can reduce the chances of their cargo's being inspected by simply submitting paperwork to Customs claiming that they have rigorous security measures in place, provided they have no history of shipping deadly cargo. The problem is that the benefit of a decreased chance of inspection is extended *before* Customs investigators get around to verifying that the security measures the companies claim to have in place are in fact in place. According to the same Senate subcommittee referenced above, less than a third (27%) of the companies in the program are validated beforehand.

Finally, when cargo containers are inspected, there is no assurance that any weapons of mass destruction within them will be found because there is too little radiation detection equipment deployed here at home and abroad at CSI ports, and the equipment that there is does not work all that well.

According to a New York Times account of the work of the referenced Senate subcommittee, only about 700 of the planned for 3,000 radiation portal monitors have been installed here in this country. At the average deployment rate last year of 22 per month, full deployment will not occur until 2009 at the earliest. Furthermore, radiation portal monitors are imperfect at best. They can detect radiation and pinpoint its location within a container, but they cannot distinguish between deadly radiation and the innocuous kind that naturally occurs in, say, kitty litter, bananas, and ceramics.

In short, then, our maritime sector is dangerously insecure. All experts agree that the likeliest way for terrorists to smuggle a weapon of mass destruction into the country would be in a cargo container bound for a U.S. port. Needless to say, a terror attack using a weapon of mass destruction could exceed the impact of 9/11 by several factors of magnitude. So, there is not a moment to waste in enhancing cargo and maritime security.

As for HR 4954, overall, I believe that it is a step in the right direction. But, in my judgment, certain provisions should be strengthened. For example, with regard to ATS, the Secretary of Homeland Security should be *required* to reduce the time period allowed by law for revisions to the cargo manifest, not just invited to consider doing so. The fact that the manifest can now be revised for up to 60 days *after* the ship arrives in the United States makes a mockery of the manifest as a targeting tool. Further, the manifest can now be written in such a vague fashion that it can likewise be rendered meaningless. Greater specificity must be required.

As for the deployment of radiation detection equipment, I believe that more than a *plan* from the Secretary should be required at this point, nearly five years after

9/11 and more than three years since the creation of the department. The money to do so must be appropriated, of course, but I would *require* the Secretary to deploy an adequate supply of radiation detection equipment to every American seaport and every foreign port from which cargo bound for the United States sets sail within a time certain, but no later than one year from enactment. We showed, in the aftermath of 9/11 that we can move at warp speed when we have the requisite sense of urgency; though, thankfully five years have passed since the last attack, there should be no less of a sense of urgency today.

And, it's not just a matter of deploying equipment. The equipment needs to work. The department's Domestic Nuclear Detection Office should move with dispatch to develop radiation detection technologies that can detect radiation, pinpoint the location of it, distinguish between harmless and harmful kinds of radiation, *and* be in compliance with the demands of the American National Standards Institute (which none of the radiation detection equipment presently used is).

As for CSI, countries should be discontinued from the program if they consistently refuse to inspect containers that we deem to be high-risk. As for CTPAT, it should become a "trust but verify" program. As presently constituted, the bill keeps it at a "verify but trust" program, by allowing companies to operate under the program for up to one year without validation. Only those companies whose security programs have been validated as rigorous should be given the benefit of a reduced chance of inspection, and the security assessment should be updated annually. This will require significantly more resources, needless to say, but homeland security cannot be done on the cheap.

Thank you, again, for inviting me, and I look forward to your questions.

Chairman KING. Thank you Mr. Ervin.

Ms. Rooney?

STATEMENT OF BETHANN ROONEY, MANAGER OF PORT SECURITY, PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Ms. ROONEY. Chairman King, thank you very much for the opportunity to testify this afternoon on the importance of port and cargo security. In the interest of making some recommendations on how to improve the bill, which we fully support, I would like to focus on six key areas: cargo security, credentialing, the importance of data, response and recovery, research and development, and finally, funding.

As has been said many times today, our goal should be to increase our level of confidence that we know exactly what is in each and every container before it has loaded on a ship to the United States.

In the Port of New York and New Jersey alone, we receive 7,600 containers a day. It is not possible to physically inspect each one of those containers here on U.S. shores, but rather, we need to continue to push the borders out.

We strongly support your proposal to establish minimum and mandatory cargo security standards. Voluntary cargo security measures such as those established under C–TPAT are helpful but not sufficient by themselves in order to protect our homeland. Rather, all containers destined to the United States should be subject to a new and higher security standard. Then and only then should importers that choose to go above and beyond the minimum standards reap tiered benefits such as those currently available through C–TPAT.

Radiation detection, which has also been talked about quite a bit this afternoon, is another line of defense. But doing that after the cargo has arrived on our shores should be our last line of defense, not our first line of defense.

We therefore support the development of a strategy for the deployment of radiation detection equipment at all U.S. ports of entry as well as in foreign ports.

But there is more to it than just picking the right sensors and establishing inspection protocol. Sensor alarming, networking, communications and response protocols should all be included in the mandated DMDO strategy.

Additionally, we must not stop at radiation detection but also address nonintrusive inspection technology and practices for the interdiction of other WMDs such as chemical and biological agents.

With regards to credentialing, we share the concerns of the World Shipping Council and RILA with regards to the Section 8 that calls for a check of all workers against the terrorist watch list.

Our concern is that imposing a new mandate on the Department of Homeland Security would shift their focus from implementing the TWIC program to another initiative, and since we seemed to have gained momentum in the last couple of weeks with TWIC, let's encourage them to keep going on that.

Accurate and reliable data—accurate, reliable, and timely shipment data is critical, not only for prevention activities such as targeting and inspection, but also for law enforcement and emergency response. Once the cargo leaves the U.S. port terminal—be it by road, rail or inland barge—the state and local law enforcement and emergency response agencies currently have zero visibility into the contents of those millions of containers that criss-cross our country every year.

Whether for commercial vehicle inspections on our highways and critical bridges or tunnels, or during a road or rail accident, this same information can prove beneficial to police and emergency response personnel in order to mitigate the damage and protect life and property.

We, therefore, support the idea or encourage the committee to consider expanding the secure freight initiative, as the secretary has talked about earlier.

We support the development of joint operation centers in key U.S. ports and facilities in order to facilitate operational control and information sharing. However, we would also recommend two changes here as well.

First, since the Maritime Ministry does not operate in a vacuum but rather is largely dependent on surface transportation and requires the involvement of multiple levels of government and public safety agencies, we believe that these operations center should not be limited to maritime and cargo security alone but be brought in to embrace more integrated, multi-disciplined regional approach spanning the broader range of homeland security functions.

Secondly, personnel resources are already stretched too thin. With technology, people no longer need to be sitting in the same room in order to achieve a common objective. We, therefore, we request the committee to consider virtual connectivity as envisioned in the port authority's on regional information joint awareness network as an alternate to a physical command center.

We also need a coherent federal vision on a national Homeland Security architecture. Absent such a vision and a set of guiding standards, we run the significant risk of local, state and federal op-

erations centers that need to work together in an emergency not being compatible with one another in technology, operational methods or both.

The SAFE Port Act creates a prioritization for reestablishing the flow of commerce in the aftermath of an incident. That is just not practical. In addition to the practical limitations, we discourage legislating a prioritization since, in a large port, a port's ability to reestablish the flow of commerce will be incident dependent and will be dictated by ongoing response or clean-up activities, current threat information, and the availability of critical transportation infrastructure and resources such as pilot's tugs, rail cars, barges, labor and so forth.

Local port officials must have maximum flexibility to respond to their specific circumstances according to the dictates of the immediate situation. In New York and New Jersey, we have developed the port recovery plan, which makes life safety and public healthy, such as home heating oil in the winter, a priority.

Thereafter, vessels will move on a first-in first-out basis, depending on the availability of infrastructure and resources.

We have also established a recovery advisory board to counsel the captain of port and unified command on a priorities requirement and limitations for an effective and efficient recovery.

With regards to research and development, it is absolutely critical that we coordinate all cargo security projects in a single office, and we support the creation of a director-of-cargo-security policy within the policy directorate.

We would, however, also encourage the development of a joint program office and a cargo security working group that would include private-sector participation.

Finally, with regards to port security funding, so far, grants have predominantly been allocated to individual projects within offense line of marine terminal or of a particular vessel. We would encourage that future grants be focused on comprehensive port needs as opposed to individual facility security needs.

Our testimony provides further detail on each of these initiatives, and we would be happy to answer questions from the committee.

[The statement of Ms. Rooney follows:]

PREPARED STATEMENT OF BETHANN ROONEY

Chairman King, members of the Committee, thank you for the opportunity to testify on ways to improve maritime and port security and the proposed SAFE Port Act. I am Bethann Rooney and I am the Manager of Port Security at The Port Authority of New York & New Jersey.

The tragic events of September 11th have focused our collective attention on the need to protect our borders at major international gateways like the Port of New York and New Jersey and small ports alike. The Maritime Transportation Security Act of 2002 is landmark legislation that has positively impacted our homeland security. However, as we all know, more remains to be done. We commend Representatives Lungren and Harman and this Committee for introducing the SAFE Port Act and a layered approach to enhancing maritime security, particularly with regard to supply chains.

This afternoon I would like to briefly discuss seven key points: (1) the vital nature of our ports; (2) cargo security; (3) credentialing; (4) the importance of data; (5) response and recovery; (6) research and development; and finally, (7) funding.

THE VITAL NATURE OF PORTS

Ninety-five percent of the international goods that come into the country come in through our nation's 361 ports; twelve percent of that volume is handled in the Port

of New York and New Jersey alone, the third largest port in the country. The Port generates 232,900 jobs and $12.6 billion in wages throughout the region. Additionally, the Port contributes $2.1 billion to state and local tax revenues and $24.4 billion to the US Gross National Product. Cargo that is handled in the Port is valued at over $132 billion and serves 80 million people, or thirty five percent of the entire US population. In 2005, the port handled over 5,300 ship calls, 4.792 million twenty-foot equivalent units (TEU's), or 2.8 million containers, which is approximately 7,600 containers each day, 722,411 autos and 85 million tons of general cargo. Today, international trade accounts for 30 percent of the US economy. Considering all this, it is easy to see how a terrorist incident in our nation's ports would have a devastating effect on our country and its economy.

CARGO SECURITY

Standards and Procedures

America's consumer-driven market depends upon a very efficient logistics chain, of which the nation's ports are just a single link. US ports provide the platform to transfer imported goods from ships to our national transportation system—primarily trucks and trains—that ultimately deliver those products to local retail outlets or raw goods to manufacturing plants. Historically, that goods movement system has had one overall objective: to move cargo as quickly, reliably and cheaply as possible from point to point. Today, a new imperative—national security—is injecting itself into that system. As such, we know that ports themselves are not the lone point of vulnerability. Rather, the potential for terrorist activity stretches from the cargo's overseas point of origin or place of manufacture to where the cargo is stuffed into a container to any point along the cargo's route to its ultimate destination.

Our goal should be to increase our level of confidence that we know exactly what is in each container *before* it is loaded on a ship destined for a US port. It is not possible to physically examine the contents of each of the 7,600 containers that arrive each day in the Port of New York and New Jersey alone without seriously impacting the efficiency of the logistics chain. Proposals for 100% physical inspection of every container entering the country are well intentioned—and wholly impractical. Such a requirement would not simply slow commerce down; it would bring it to a halt. The key is to find a way of separating high-risk cargoes from the vast majority of legitimate containers and then dealing with the exceptions. This approach requires a systematic understanding of the logistics chain that now moves that container from any place in the world to the distribution system in our country.

A typical container movement includes 14 different nodes, involves 30 organizations, and generates as many as 30–40 different documents with over 200 data elements. This is a complex process in which the physical movement of a container is only one major dimension of the system. There are three other important components that must also be understood: the flow of money, the flow of information and data for that shipment, and, finally, the transfer of accountability, all of which must occur seamlessly in order for the cargo to be delivered to its final destination.

Today, there are no mandatory security standards when loading a container at the manufacturer or when it is consolidated in a warehouse, often well inland of a seaport. There are no security standards for the seals that are put on containers. Cargo is transferred from one mode of conveyance to another and there are neither standards for how that is done nor accountability for the integrity of the container as it changes hands.

We believe that efforts must be taken to verify the contents of containers before they are even loaded on a ship destined for a US port. The process must include certification that the container is free of false compartments, was packed in a secure environment and sealed so that its contents cannot be tampered with, that there be an ability to verify along the route that neither the container nor cargo has been tampered with, that it is transported under the control of responsible parties, and that the integrity of the information and information systems associated with the movement of the cargo has not been compromised.

We strongly support your proposal to establish ***minimum and mandatory*** cargo security standards. Voluntary cargo security measures such as those established under the Customs-Trade Partnership Against Terrorism (C–TPAT) program are helpful but are not sufficient by themselves in order to protect our homeland. Rather, all containers destined to the United States should be subject to a new and higher security standard. Then and only then, should importers that choose to go above and beyond the minimum standards reap tiered benefits such as those currently available through C–TPAT participation. The incentives to go above and beyond the minimum standards would be commensurate with the level of investment in and effectiveness of security measures and should also generate a number of security and commercial benefits including a reduction in cargo loss, fewer Customs exams, an adjustment to insurance premiums and bonding requirements and greater cargo visibility to support just-in-time inventory pressures.

Weapons of Mass Destruction—Radiation Detection

Radiation detection is yet another line of defense but radiation detection in the United States after cargo has arrived on our shores, should be our last line of defense, not our first. We support the development of a strategy for the deployment of radiation detection equipment at all US ports of entry. However, in addition to deploying radiation detection equipment at US ports, similar capabilities must be available at Container Security Initiative (CSI) and other foreign ports as well.

The Port Authority has been working with the Department of Homeland Security (DHS) since 2003 on a Counter Measures Test Bed (CMTB) program to test and evaluate the performance of commercially available and advanced radiation detection equipment in real world situations. Our efforts have focused on the development of better standard operating procedures and an assessment of the impact on the flow of commerce. We have learned through the CMTB that it is not just about sensors and inspection procedures but also sensor alarming, networking, communications and response protocols all of which should also be included in the mandated Domestic Nuclear Detection Office (DNDO) strategy. Additionally, this legislation should not be limited to radiation inspection/detection but must also address non-intrusive inspection and sensor / trace detection practices, procedures and technology for the interdiction of other Weapons of Mass Destruction, especially chemical and biological agents in a shipping container. Testing a container and its cargo for chemical or biological contamination presents different technological challenges than for a passenger passing through an airport security checkpoint. We must urgently pursue a solution that is easy to administer by our supply chain workforce, is fast, accurate and reliable, and is affordable.

CREDENTIALING

In 2002, Congress mandated that all transportation system workers who are permitted "unescorted access" to restricted areas carry a Transportation Worker Identification Credential, or TWIC. TWIC is a tamper resistant identification card with biometric capabilities that can be issued only after a successful criminal history background check. TWIC provides the operators of critical infrastructure with the ability to positively identify an individual seeking to gain access to a secure area. We fully support the need for positive access control at port facilities and the creation of a national identification program.

We have concerns about Section 8 of the SAFE Port Act which requires States to submit biographical information on all people requiring access to secure areas for comparison to the terrorist watch list. This new requirement could divert the Department's much needed attention from the creation of TWIC and, as currently drafted, it fails to provide port authorities and terminal operators with a methodology (*i.e.* a database and identification cards) to verify that an individual has indeed been checked against the watch list. The provisions of Section 8, could, if not altered to address the flow of container traffic, create major delays at our ports and terminals, thus affecting productivity and the economy. We urge the Committee to continue to work with the Department of Homeland Security to quickly implement the TWIC program nationwide and are encouraged by recent development including the release of a Request for Proposals (RFP) and indication that the Notice of Proposed Rulemaking (NPRM) can be expected in a matter of weeks. Let's keep this new momentum going and not start on something new.

IMPORTANCE OF DATA

Improvements to the Automated Targeting System

As mentioned earlier, there are close to 200 data elements associated with a shipment from origin to destination. This data is critical not only for prevention activities such as targeting and inspection, but also for law enforcement and emergency response. We need to provide Customs and Border Protection (CBP) more complete and accurate data earlier in the chain of custody for targeting and inspection purposes. We also must be able to provide this data, or a subset thereof to other federal state and local law enforcement and emergency response agencies.

The primary information that CBP uses in its Automated Targeting System (ATS) is the carrier's bill of lading or manifest which is provided to CBP 24 hours before a ship is loaded in a foreign port. The carrier's manifest data has limitations and should be supplemented with additional commercial data from the US importer or foreign exporter before the vessel is loaded in order to strengthen the risk assessment process. Today, the more comprehensive cargo entry data is not required to be filed until after that cargo has already arrived in the US, often at its final destination well inland of our ports—too late to be used for screening and inspection purposes.

The Port Authority was a member of a Customs Commercial Operators Advisory Committee (COAC) sub committee last year which recommended that importers pro-

vide CBP with advance entry data before vessel loading. While we understand that DHS and CBP are still considering this important change, it has gotten little traction. We support your provision to improve the Automated Targeting System and believe that this can be accepted by the industry in relatively short order since COAC, an industry wide advisory group, has already evaluated it and provided specific recommendations. CBP must be provided with both the financial and personnel resources for this to be effective; therefore, the Committee should authorize sufficient funding for this critical program.

Uniform Data for Government-Wide Usage

In addition to making import and export data available to other federal agencies, we encourage the Committee to also include state and local law enforcement and emergency response agencies as well. While this data is useful to federal agencies for screening and inspection purposes, once the cargo leaves the US port terminal, be it by road, rail or inland barge, the state and local law enforcement and emergency response agencies currently have zero visibility into the contents of those millions of containers. Whether for commercial vehicle inspections on our highways and critical bridge and tunnel crossings such as the Port Authority's own George Washington Bridge and Lincoln Tunnel or during a road or rail accident, this same information can prove beneficial to police and emergency response personnel in order to mitigate damage and protect life and property.

RESPONSE AND RECOVERY

While much of the focus since 9/11 has rightfully been on preventing another terrorist attack; we must develop comprehensive programs to address response and recovery as well.

Joint Operations Centers

One of the principal outcomes of the work of the 9/11 Commission was the determination that information sharing and collaboration at all levels of government were less than adequate. As such, we support the development of joint operations centers in key US ports to facilitate operational coordination, information sharing, incident management and effective response. However, we do not support the implementation of regional or port-wide Joint Operations Centers exclusively for maritime and cargo security as currently outlined in the SAFE Port Act. The maritime industry does not operate in a vacuum but rather is largely dependent on surface transportation (road and rail) and requires the involvement of multiple levels of government and public safety agencies. Each of these agencies have information networks and operations centers of their own that must be staffed and supported which are expensive to maintain in both personnel and infrastructure. A new port Joint Operations Center would require personnel from agencies already stretched to the limit. Theerefore, any new Joint Operations Center created through this legislation should not be limited to maritime and cargo security alone but be a single focal point and provide for the integration of all Homeland Security related functions among local, state and Federal agencies in a given region. It must also not just be a single center but a coordinating node in a regional and national information sharing and collaboration network linked to other operations centers.

Over the last several years, hundreds of millions of dollars in Federal Homeland Security funding has been spent to develop and implement disparate information sharing networks and joint operations centers at the local, state and federal levels without the benefit of a coherent federal vision on a national homeland security architecture. Absent such a vision and a set of guiding standards, we run the significant risk of local, state and federal operations centers that need to work together in an emergency not being compatible with one another in technology, operational methods or both.

There are three promising efforts now underway that we recommend the committee consider in its deliberations over the Joint Operations Center provision of the SAFE Port Act. The first is the National Command Capability Working Group, a Joint DHS/DoD program to set direction for a national information sharing and collaboration network. The second is a program called Joint CONUS Communications Support Enterprise (or JCCSE), a joint project of US Northern Command and the National Guard Bureau. The third effort is the Regional Information Joint Awareness Network or RIJAN. RIJAN is a DHS funded, DoD managed and Port Authority led multi-agency project to build an information sharing and collaboration network among key operations centers in the New York and New Jersey port region. Regional partners include the States of New York and New Jersey and the City of New York. DHS sponsorship is via the Domestic Nuclear Detection Office (DNDO). Our DoD program manager and developer is the US Army's Communication Electronics Development and Engineering Command from Fort Monmouth New Jersey.

The Joint Operations Center provision is a very important part of the SAFE Port legislation. However we encourage the sponsors and this committee to seriously consider modifying this provision to broaden its scope and embrace a more integrated, multidiscipline, regional approach spanning a broader range of Homeland Security functions and interests within port regions. Doing so will help simplify overall Homeland Security networking and information sharing by avoiding duplication, it will be more efficient in terms of staff and infrastructure, and it will go a long way to enabling a DHS vision for a unified approach a national information sharing and collaboration architecture. Prior to nationwide implementation, we strongly recommend that the SAFE Port Act support the funding and development of at least two comprehensive port region Joint Operations Center demonstration projects. The Port Authority, with a prototype regional communications network already established stands ready to partner in such a Joint Operations Center test bed program.

Recovery and Economic Impact

A large-scale terrorist attack at a Port such as ours would not only cause local death and destruction, but could paralyze maritime commerce and economies nationally and globally. In advance of such an event, we must have plans in place to ensure an efficient and effective response in order to avoid critical delays in recovery and business resumptions. Agencies in the Port of New York and New Jersey know better than anywhere else in the country how to respond to suspected terrorist activities and catastrophic events. What is not entirely clear is how private sector resources could be leveraged to strengthen the response, what the economic impact of a protracted port closure would be, and how the private sector would be kept informed to facilitate critical business decisions as an event unfolds. We must collaborate today on developing plans and procedures to ensure a timely and effective recovery from an incident at our Ports and to keep the private sector informed, many of whom are not physically located in the region, as an incident develops and response and recovery takes place.

Through the Area Maritime Security Committee, the Port of New York and New Jersey has developed a draft port recovery plan. We have also established a Recovery Advisory Board to counsel the Captain of the Port and Unified Command on the priorities, requirements and limitations for an effective and efficient recovery. A crucial element however, before we can finalize our port recovery plan is the release of the Maritime Infrastructure Recovery Plan or MIRP by the Department of Homeland Security, one of eight supporting plans of the National Strategy for Maritime Security.

The SAFE Port Act creates a prioritization for reestablishing the flow of commerce in the aftermath of an incident. We discourage legislating a prioritization since in large part, a ports ability to re-establish the flow of commerce will be incident dependent and be dictated by on-going response or clean up activities, current threat information and the availability of transportation infrastructure and resources (pilots, tugs, rail cars, barges, labor, cranes, tankage, container storage, etc.). Local port officials must have maximum flexibility to respond to their specific circumstances according to the dictates of the immediate situation. The recovery plan for New York and New Jersey makes life safety and public health, such as home heating oil in the winter, a priority; thereafter, vessels will move on a first in first out basis depending on the availability of infrastructure and resources.

It is not practical to give priority to vessels that have a security plan approved by the Coast Guard, are entering the US directly from a CSI port, are operated by validated C–TPAT participants, or are carrying Green Lane designated cargo. While a vessel may have sailed directly from a CSI port, it likely would have called at three or more ports on that voyage, some or all of which may not be CSI ports and therefore the cargo may not have been physically verified before loading. Also, a ship could have upwards of one thousand containers on board that are expected to be offloaded in a particular port, only a fraction of which might be Green Lane designated cargo. Once loaded on a ship, there is no way to segregate or prioritize Green Lane from non Green Lane cargo.

RESEARCH AND DEVELOPMENT

It is absolutely critical to coordinate all cargo security research and development efforts through a single office and we support the creation of a Director of Cargo Security Policy. [KRT1]Today, cargo security projects are being managed by various agencies within DHS as well as DOT, DOD and DOE. There are also a number of private sector cargo security initiatives that should be monitored by the same central office. From our vantage point, there is little coordination and collaboration among all these initiatives. As a result, we may be expending scarce research resources in duplicative efforts or pursuing technologies or devices in one program that have already been shown to be ineffectual in others. We risk reinventing the

wheel in developing solutions already encountered and solved in other efforts. Erecting administrative barriers between these programs impedes the free exchange of information that could otherwise promote efficiency and effectiveness in improving security.

A positive example can be found in Operation Safe Commerce, a government-industry initiative to study maritime supply chain security. Along with our sister ports in Seattle-Tacoma and Los Angeles-Long Beach, we have participated from the beginning in evaluating various approaches to improving supply chain security into our ports. The sharing of information and experiences between the ports has been a key element in achieving maximum return on our investment in time, money, and results. It has ensured we do not duplicate efforts being evaluated in the other ports. At the same time, we recognize there are challenges common to all of us regardless of the solutions being studied. The experience of others has enabled us to quickly resolve certain issues while offering our own experience in other areas to our sister ports for their benefit. Further promoting the concept that the experiences of a few can benefit the many is the presence of an Executive Steering Committee to monitor the progress of the study participant and involve those government departments and agencies with a stake in this important effort. Outside Operation Safe Commerce, however, we have virtually no insight to other initiatives with similar objectives such as the Smart Box and Advanced Container Security Device programs.

There is an old saying that ignorance is bliss. In the current context, however, ignorance is an obstacle. Improving our national security is not a competition between government contestants seeking to conceal information in order to gain an advantage over other contestants. Rather, those of us involved in these efforts should be players on the same team working for the common good. In addition to the creation of a Director of Cargo Security Policy, we would encourage the development of a Joint Program Office and a cargo security working group that includes private sector participation.

FUNDING

Port Security Grant Program

Clearly there is an on going debate over whether port security is a federal government or private sector responsibility. While that debate continues, the Port Authority and private terminal operators throughout the country have willingly taken significant steps to protect our seaports from the new terrorism threat, because the consequences of not doing so are grave. Since September 11th, ports such as ours have instituted heightened security measures and spent significant amounts of money to increase security, both with capital improvements and additional security and law enforcement personnel. However, for every dollar that is spent on security, there are ten fewer dollars that can be spent on the capital infrastructure that is required to accommodate the increasing volume of cargo that our ports are expected to handle.

In an attempt to provide you with a sense of the scope of the challenge we face, I offer two possible indicators of local port needs.

Since June 2002, when the first round of Port Security Grants was made available, terminals in the Port of New York and New Jersey have applied for over $200 million in Federal assistance. Of the $707 million that has been appropriated for port security grants across the country, a total of $53.7 million, which is just 7.5 percent of the total, has been awarded to entities in our Port. The Port Authority itself has submitted requests totaling $42 million, but has been awarded only $10.5 million, including $2.3 million for technology demonstration projects which the Port Authority sponsored on behalf of the federal government, or just 25% of the identified need.

In the Coast Guard rulemaking, it was estimated that the cost for port facilities throughout the country to implement the Maritime Transportation Security Act (MTSA) over the next decade would be $5.4 billion. Given the required cost share for federal grants of twenty—five percent, by the Coast Guard's own estimate, it would require $400 million a year in federal assistance in order for ports and terminals to adhere to the MTSA. Despite this, only $175 million was allocated nationwide for port security in FY 2006. That is significantly more than was requested in the President's budget, but still far short of the need that America's ports have identified.

While these grants help defray the cost of some physical security measures, such as access control, intrusion detection, fencing, lighting, identification systems, CCTV and gates, there has also been a significant increase in the operational costs associated with maritime security as well. It is estimated that the annual operations and maintenance costs associated with the new security systems is on the order of mag-

nitude of fifteen to twenty percent of the purchase price. Additionally, ports and terminals have spent significant sums of money on personnel related costs, including the hiring of new security officers, overtime, upgrading security forces to use more professional services, and for providing extra training. The Port Authority's port security operating costs have doubled since 9/11. This does not include the extra police that are required at all Port Authority facilities every time the threat level increases, which amounts to approximately $500,000 per week.

The vast majority of the $707 M in port security grants has been allocated to critical security projects for individual terminals and vessels. Since all US port terminals and vessels are now compliant with the Maritime Transportation Security Act, we must shift our attention from "my" security needs to "our" security needs. We therefore support the provision to make grants available to address vulnerabilities identified in the Area Maritime Security Plans (AMSP). Further clarification however is needed to define who and what kinds of entities can apply for grants on behalf of the port area or region as well as well as understanding the parameters around our federal partners such as the Coast Guard receiving benefits from projects funded through these grants.

CONCLUSION

Addressing the issue of port and maritime security is an enormous challenge given the complexity of the international transportation network. Devising a system that enhances our national security while allowing the continued free flow of legitimate cargo through our ports will not be solved with a single answer, a single piece of legislation, or by a single nation. It will require a comprehensive approach with coordination across state lines and among agencies at all levels of government as well as the cooperation of the private and public sectors and the international community. Importantly, it will require additional resources for the agencies charged with this awesome responsibility and for the public and private ports and terminals where the nation's international commerce takes place.

I hope my comments today have provided with you some helpful insight into this complex matter. We at the Port Authority of New York & New Jersey are prepared to offer any additional assistance that you may require. Thank you.

Chairman KING. Thank you very much to each of you for your testimony. I have a series of questions.

I have some of Mr. Ervin. I will start with you.

In your prepared testimony, you talk about the radiation portal monitors, and it appears there might be an inconsistency in your testimony, but I will let you clarify it. Well, you say that they are imperfect at best, then you urge rapid deployments of these radiation portal monitors. I guess my question would be: If the technology is not as good as you feel it should be, why should we rush to deploy them?

Mr. ERVIN. I think what I said, Mr. Chairman, or at least what I meant to say is that on the one hand, we are not getting these radiation portal monitors into our ports as quickly as we should. We are way behind schedule, as GAO has acknowledged, but even if we were to do that, the technology is limited at best. As I say, radiation portal monitors are good in that they can identify radiation, and, unlike these personal radiation detectors which can merely detect radiation, RPMs can actually pinpoint the location of the radiation inside the container. They can isolate, but they cannot distinguish between the deadly kind of radiation and the harmless kind. Only radiation isotope identifier devices can do that.

And I have heard no talk about the deployment of those on a wide-scale basis in the department. And that said, even that last device, RIIDs, all four of these systems—a personal radiation devices, the RPMs, the RIIDS, and there is one other device as well that is very much like the first one—none of these meets the standards of the American National Standards Institute.

There was a memo that went out last year from the applicable office in the Department of Homeland Security that said that. So we need this next generation of equipment. We need it desperately. And it seems to me that if a sufficient amount of money were designated for this purpose, then we could redouble our efforts to develop it and to deploy it just as quickly as possible.

Chairman KING. There were several points where your testimony diverged from Mr. Jackson, certainly on the 17.5 percent. Let me just ask you, let's assume that everything you are saying is true. Is it possible—and what Mr. Jackson is saying is true. Are we talking about a difference in philosophy? Are we talking about a lack of ability?

And I don't mean this in an argumentative way. Why do you think there is this difference of opinion between you and Mr. Jackson? Is it a philosophical difference? Is it something that can be addressed? Is it just they are not getting the job done?

Mr. ERVIN. Well, I think it is frankly, that they are not getting the job done. I don't think it is the philosophical difference. And by the way, sir, these are not my statements. Everything that I have said is based on, either, as I say, on inspector general report, a report of the GAO, or a report—

Chairman KING. I am assuming, for the purpose of the hearing, everything you are saying is true. I am just asking why you believe that is true then.

Mr. ERVIN. Well, I don't know other than that my sense is the department wants to suggest, frankly, that we are better off than we are. I mean, to continue to say that we are screening 100 percent of the cargo suggests, as I say, to the average person that we are inspecting 100 percent of the cargo. In fact, we are not. And we are not even doing what we claim to do. Screening simply means, as I say, assessed. We are not doing a hundred percent of that. Thirty-five percent of the time, we have no assessment whatsoever of this cargo.

So I think the very beginning thing that the department needs to do is to acknowledge what is true and what is not. We need to acknowledge that we don't know anything about a third of the cargo that comes into the country. We need to acknowledge that with regard to the two-thirds that we are assessing, 20 percent of it is not being inspected abroad at these CSI ports even though we are requesting the foreign governments to do that. And it seems to me that we should get rid of the CSI program if there is this kind of noncompliance rate.

Certainly, in a country like France, which is supposed to be an ally of the United States, if 60 percent of the time our intelligence analysts tell us that there is something dangerous in the cargo, and France, notwithstanding that, refuses to inspect it, at a minimum, it seems to me, France should be dropped from the CSI program.

And furthermore, as I say, the good news is supposed to be that in those instances where foreign countries don't inspect cargo, it is supposed to be inspected here when it gets here, never mind that the whole point of CSI is to do it beforehand, because it might be too late when it gets to this country. At least 7 percent of the time it is not inspected here in the United States as well.

With regard to C–TPAT, which we haven't even talked about yet, it seems to me that that program likewise should be done away with. If we are giving these benefits before we are validating that the companies are actually—that they actually have in place the security programs they claim to have in place, it is a huge potential for Trojan wars.

Chairman KING. If Mr. Pascrell will indulge me, I would like to ask each of the other three panelists if they would comment on those observations. And I am not doing this simply to provoke a debate. I would be interested in your comments on this. I really would be interested in your comments on it.

Mr. KOCH. Mr. Chairman, I don't know where Mr. Ervin's 35 percent comes from. I am sure there is a basis for it. Our carriers carry containers into the U.S., file with the U.S. government 24 hours before vessel loading all the data they have on every container that is shipped to the U.S. So as far as I know, in terms of containerized shipments moving in on vessels, it is 100 percent of screening.

It is important to distinguish between screening and inspection, and we do suffer from terminology problems even in this hearing today at times on this particular issue. We do fully agree that better data would be appropriate to acquire so that screening process is a better process. And as we have stated in our testimony and over the last several years and continue to advocate that.

As to the question about cooperation in foreign ports, I would simply observe there is an easy solution if we are not getting cooperation from a foreign customs authority. And that is, U.S.Customs can just tell the carrier not to load the box. There is no ocean carrier that would not be very happy to abide by a request from Customs not to load a container on one of its ships coming to the U.S. if the U.S. government thinks that there is a security risk significant enough to warrant a do-not-load vessel. So there is a self-help mechanism that CBP has here, and anytime it would like to use it, and our carrier members would absolutely implement that, until whatever the issue it was that generated that request could be resolved in conjunction with the foreign government.

Ms. ROONEY. Mr. Chairman, I think—I am also not familiar with that 35 percent number that Mr. Ervin refers to, but I would suspect that also it is the non-containerized cargo which points to an issue in and of itself. Our programs post–9/11 have been container centric. They have been focused on the containerized trade and there has been little in terms of focus on roll-on roll-off cargo and other bulk-type commodities.

So whatever that 35 percent number comes from, if that is, indeed, non-containerized cargo, then we need to move from containerized programs and start beginning to focus on non-containerized cargos as well, because they pose a risk.

Chairman KING. Mr. Gold?

Mr. GOLD. I don't think I have much more to add. I think both Chris and Beth both addressed the question very appropriately. I think, you know, we need to continue to work on improving the CSI program, make sure that container screenings and inspections are done when they are requested by Customs and Border Protection,

and again, focus on making sure that we do have the right information to do the targeting in advance of the containers being loaded.

Chairman KING. Mr. Ervin, you can comment, and Mr. Pascrell.

Mr. ERVIN. Thank you very much, sir. This is containerized cargo we are talking about. It is non-containerized cargo. And I am surprised at my colleagues on the panel have not heard of this report upon which my statement is based. It is a GAO report from just last year. So I would urge them to read it, because it says what I claim it says.

Chairman KING. The gentleman from New Jersey, Mr. Pascrell.

Mr. PASCRELL. I was just handed, Mr. Chairman, the report that I think Mr. Ervin is referring to, which came out last year in April of 2005, which is you are using your statistics from the GAO report. I will enter it into the record.

Mr. ERVIN. Thank you, sir.

Mr. PASCRELL. I would say that we have a little problem here. I think we need to pass this legislation right away, but if there is a conscious effort to confuse the Congress and establish a false sense of security, it wouldn't take too much to confuse us, but if that is—Congress must use its oversight power, it would seem to me.

Now I would like your opinion, Mr. Ervin, of what Mr. Gold said in his testimony. Mr. Gold said that the Retail Industry Leaders Association supports 100 percent screening of high-risk containers, of high-risk containers. But a policy requiring 100 percent scanning of all U.S.-bound containers is neither effective as a deterrent nor feasible operationally as a security enhancement measure. Would you give me your opinion of that?

Mr. ERVIN. Absolutely, sir. First of all, if that is in fact what Mr. Gold said, to claim that it is sufficient to have 100 percent screening of only high-risk cargo, is less than the department now touts. Department claims that there is 100 percent screening of all cargo.

Mr. PASCRELL. Which is not true.

Mr. ERVIN. Which is not true, but at least they claim that there is 100 percent screening of all cargo. Mr. Gold is saying he supports or the organization supports a 100 percent screening of only high-risk cargo that they lower the threshold when they are already low, an erroneous threshold, that the department has set for itself. That is the first point.

Secondly, with regard to 100 percent screening is neither effective nor a deterrent, well, I don't know how I can respond to that, because if there really is 100 percent inspection of cargo, it seems to me, that is the only way to inspect it—to either physically open it up or to do it in a nonintrusive way, that is the only way to determine what the contents are.

Mr. PASCRELL. Well, we—

Mr. ERVIN. So it would be awfully effective if we were to do this.

Mr. PASCRELL. If we inspected every container, we would send commerce out into the oceans. You understand that. But let's not kid ourselves into thinking that we are doing what we are saying what we are doing, and I think the GAO report in April of last year was very clear about that.

You know what this reminds me? There is an argument going on in the Congress, if I may, Mr. Chairman. There is an argument going on in the Congress now about screening or examining the eyes of poor children in this country, going through examination. And some folks are satisfied with screening. We know that so many young kids fall through the cracks when that happens. Unless you give a person an examination, an eye examination, you are never going to be able to detect nor prescribe a remedy. This reminds me so much of that. I know it is apples and oranges, but just—it came to my mind.

This is serious. Not only is this a surrender to the language, there is something more important here than just screening and scanning and inspecting and examining. We know that game. There is something more hideous here to me, because not only do you establish your false sense of security, we are not doing what we are saying we are doing.

Mr. ERVIN. That is the point I am making. And just to finish, the whole business about it not being feasible operationally, we have pointed out that it is happening in Hong Kong, which is the busiest port in the world. It, according to the experts, can be done in a very, very cost-effective fashion. And further, the department says it has a fiscal—doing 100 percent inspections within 2 or 3 years here in the United States with regard to cargo that comes into the United States before it goes out elsewhere in the country. At a minimum, it seems to me, the department should set the same goal and same timetable with regard to cargo that comes into the United States.

Mr. PASCRELL. Mr. Chairman, I think your legislation is very important, but something, if I may, if you will allow me license. More important than legislation, believe it or not, there is something more important than legislation, and that is that I think that there has been a universal attempt to precipitate a conclusion in us in the Congress on the committee that things are much more advanced than they really are.

I didn't get, did you, from the Homeland Security either today or in the past, a sense of urgency about this. And I believe, Mr. Chairman, we have talked about this in the past, the shipment of nuclear weapons, nuclear materials—you have spoken to that too—the shipment of nuclear materials is a very, very dangerous business. We can't afford to be half right nor accept empty conclusions from a department that at times vacillates between dysfunction and God knows what. We should all be on the same page.

This is not a party fight here at all. This is, "we want to do the best that we can." And I am telling you, I am examining all of you, and I know you are all trying to do the best in your own areas regardless of where you are. And I am familiar with the Port of Authority in New Jersey and the great job that you folks do. But I think we need to pay very much attention.

You work for Aspen now, right?

Mr. ERVIN. Yes.

Mr. PASCRELL. What title did you have in Homeland Security? Inspector general?

Mr. ERVIN. I was the—

Mr. PASCRELL. What did you have to do in that—what does that mean, that title? That is another nice title but what does it mean?

Mr. ERVIN. The inspector general is in charge of conducting inspections, audits and criminal investigations to make sure the departments are running as effectively, officially and economically as possible.

Mr. PASCRELL. Were you in the department when this was provided by the GAO which I enter into the record again, Mr. Chairman?

Mr. ERVIN. No, sir, I was not. I left in December of 2004, but I am intimately familiar with that report, and I commend it to everyone.

Mr. PASCRELL. Okay, we are going to get this around to make sure every member has it, because I think it is important, not because of what you say or what I say, but these folks, I think, provide an objective review.

Thank you, Mr. Chairman.

Chairman KING. The gentlemen from California?

Mr. LUNGREN. Thank you, Mr. Chairman. I just might say our friend from New Jersey is too humble, because I doubt that even the administration could try and get anything past you.

Mr. Koch, it appeared to me that you wanted to say something just a moment ago, and even though it is out of my time, I would love to hear what you have to say.

Mr. KOCH. I would like to clarify a comment that was just made about the Hong Kong ICIS project, which is nobody should be under the impression that it is inspecting anything. It is not an operational system. It was a pilot program that is showing technology exists to do a radiation scan and a gamma ray scan on a box. Nobody is doing anything with those images. What it is showing is that a technology does exist that can have application in the future and can be a very valuable tool, and it is a very attractive idea, but to say that Hong Kong is inspecting a hundred percent of boxes is simply an incorrect statement.

And there are a lot of difficult issues that have to be addressed when you try to roll this out into an operating strategy. The first is: What does a scan mean? Are we talking just radiation? Are we talking gamma ray of boxes? They are two different technologies.

And, for example, in the Sail Only If Scanned bill, that bill doesn't define what it is that it is talking about. Is it talking about radiation scanning, or is it talking about doing gamma ray images, or is it talking about doing both?

The second issue: Who is to do the scanning? We just had a debate in the Congress that basically said, Dubai World Ports is no longer a trustworthy entity. Is Hutchison Whampoa and Dubai Ports going to be asked to do this scanning, or are we asking foreign governments to do this scanning abroad? That is a very important question. It would have to be addressed if the Sail Only If Scanned bill is to be something that is passed.

And then the real hard issues come. When you have this image that the technology will produce or images?okay, the questions are: What do you do with this? How is it transmitted to the U.S. government, and what do they do with it? When you go through an

airport and they scan your luggage, it is a couple cubic feet of space.

When you scan a 40-foot container that has 2,700 cubic feet of space in it, it takes a trained eye 4 to 6 minutes to look at one of those scans with the shipping documents to make an assessment of what it is they are looking at. If the understanding is that a hundred percent of the boxes are going to take this technology, process it, have Customs analyze every one of those issues before vessel loading, we are going to stack up foreign ports quite a ways, which is why we come back to risk assessment.

We continue to believe that risk assessment is an important piece of this, and the tools available to CBP have to improve so we have more confidence that we are inspecting the boxes that are appropriate to inspect, but we don't think every load of Heineken coming into the U.S. needs to go through an inspection.

Mr. LUNGREN. It used to go through inspection when it wasn't in containers.

Mr. KOCH. Used to get—

Mr. LUNGREN. If you recall what?I grew up in a port city, and I used to hear the expression, "10 percent is ours." I think you know what I am talking about.

[Laughter.]

Mr. Ervin, I am intrigued by your comments but somewhat confused by your comments. Our bill is an attempt to try and build on the foundation we believe has been established by the administration to do it the better, more intensely and to bring it up to more maturity more quickly. But I am trying to find out if you believe that there is anything that has improved the security in our ports over the last number of years.

Mr. ERVIN. Well, Congressman, certain things have been done, certain. I mean, there are more personal radiation detection devices than there were before 9/11. There are more radiation portal monitors than there were before 9/11.

Mr. LUNGREN. But you have told us that they are imperfect at best. They cannot distinguish between deadly radiation, innocuous kind that naturally occurs in kitty litter, bananas, and ceramics.

Mr. ERVIN. And that is right.

Mr. LUNGREN. Well, but my question is, if that is the case, what good does it do for us to have more of them out there so that we have more false positives?

Mr. ERVIN. Well, sir, it is improvement in the sense that we have more stuff than we had in the past, but we don't have nearly what we need to have in order to be as safe as we should be. So I mean to say it would be inaccurate to say we have done nothing since 9/11. If the question is: Have we done nothing since 9/11, the answer to that is no. But that is not the issue. The issue is: Are we as safe as we can be, and are we safe as we claim to be?

Mr. LUNGREN. But I am still trying to get this from your testimony. You have criticized the effort, because we are too slow in putting radiation portal monitors in and yet you have said that they don't do much good. That would be like saying that we should have more X-rays out there and have more chest X-rays, everyone, though they are so vague they are going to have a lot of false positives. I just?

Mr. ERVIN. May I just answer—

Mr. LUNGREN. Wait a second. Mr. Jackson's approach was that because we have—we are on the eve of having better technology, he has to balance, in terms of a world in which we don't have unlimited funds, between how you go forward with putting those portals that we do have now in place versus expanding to have them there much faster even though it might be a better judgment to have those funds go to the new technology that is in the offing if, in fact, it is in the offing.

Mr. ERVIN. Well, sir—

Mr. LUNGREN. Is that a responsible position or is it totally irresponsible?

Mr. ERVIN. Well, I don't see where the inconsistency is in the testimony, frankly, Congressman. What I say on the one hand is, we claim to have radiation portal monitors in place and we do, but we are not deploying them as fast as we claim to deploy them. At the rate that we are going, it will take 3 more years to deploy them with the goal that we have. But even if we were to that that, I say furthermore, radiation portal monitors are imperfect at best.

That is not inconsistent. It is just to say, we are not doing as fast enough what we claim to be. One of the best solutions we have right now and it as a solution is not very good. That is not inconsistent, it seems to me.

Mr. LUNGREN. Can I ask you about the C–TPAT?

Mr. ERVIN. Please.

Mr. LUNGREN. You call the Customs Service disingenuous and touting it as a cargo security measure. Is that because the concept is flawed, or is it because one part of it allows for some point scoring to take place if people just sign up and send in their plans before they get the verification of that?

Mr. ERVIN. That is the concept, sir. The concept is that a company simply signs paperwork claiming that they have rigorous security measures in place. And simply because the paperwork is submitted, the benefit of reduced inspection is provided before any independent validation is done to ensure that the company does, in fact, have a program in place. That is disingenuous to claim—

Mr. LUNGREN. So your criticism is of the first part of program, not where they go to validation, because according to their figures as of the end of last year, they had completed 25 percent validations and they had 41 percent of the C–TPAT participants validations in progress—

Mr. ERVIN. I think the figures—

Mr. LUNGREN. —go up to 66 percent.

Mr. ERVIN. Yes. I think the figures, sir, is 27 percent. They have validated only 27 percent of the companies in the program. It is a simple point and the point is this. In the age of terror, should it be sufficient for a company simply to be able to say that, "We have a rigorous security measure in place," for that company to obtain the benefit of a reduced likelihood of inspection? And my answer to that is no. And it seems to me there could be no argument about that.

Mr. LUNGREN. You would support third-party verification?

Mr. ERVIN. Absolutely.

Mr. LUNGREN. Good.

Mr. ERVIN. And furthermore, I would not have the program at all if the validation can take place before the benefit is provided. I would have validation beforehand. Rather than a trust-by-verify program, it is a verify-by-trust program. And in the age of terror, we cannot afford that, it seems to me.

Mr. LUNGREN. Thank you.

Chairman KING. Gentleman from North Carolina?

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Let me thank each of you for being here today. I appreciate your comments, and I am going to try to ask concise questions and hope you can do the same with answers since the time is limited.

And Mr. Koch and Mr. Gold, these questions are for you first, please.

Thus far, most of our conversation has been focused on the megaports that we did in western commerce. Would you say that this detention has served to improve security conditions at these ports?

Mr. KOCH. At the large ports, sir.

Mr. ETHERIDGE. Yes.

Mr. GOLD. I would agree.

Mr. ETHERIDGE. You agree? What about smaller ports such as those in central South America as well as Africa?

Mr. KOCH. I believe the poorer countries are slower in getting up to speed. Certainly, some of the Caribbean ports are poor ports. And I know there is a concerted effort to try to do capacity building in those places. The Coast Guard's international port security program is visiting ports in the Caribbean and in Africa to try to assess how they are doing. And I think they are trying but they are slower.

Mr. GOLD. I would agree. We were doing business with some of those ports. We are also looking at how do we help push those ports along working with the carriers and with the governments, especially the foreign governments, making sure that they do bring their security policies up to par with what has been put in place under the ISPS code.

Mr. ETHERIDGE. Given that answer, in your estimation, which areas are the most concern due to local corruption and lack of government support?

Mr. KOCH. I don't have a specific answer for that, Congressman. I mean, there is—in some parts of the world corruption is endemic, including the customs authorities, but I don't have a specific answer as to which countries that would be.

Mr. ETHERIDGE. But you deal with it, do you not? Doesn't your association deal with it?

Mr. KOCH. Well, yes, there are interactions with those that our members have, yes.

Mr. ETHERIDGE. Mr. Gold?

Mr. GOLD. I don't know that I can answer that specifically. Didn't have direct contacts with them so I couldn't answer that.

Mr. ETHERIDGE. It seems to me that if we are talking about port security, we are talking about port security. And those growing areas where a lot of commerce is coming through and it has been redirected, it would seem to me for security issues for the United

States—because that is what we are talking about—seems like that is an area of tremendous vulnerability. Would you not agree?

Mr. KOCH. It is certainly a potential vulnerability there, and it ought to be something that the government is including in their targeting system so that when goods are originating from a higher risk part of the world, they get a higher score from the Automated Targeting System.

Mr. ETHERIDGE. Ms. Rooney, let me ask you one very quick—we talked about the scanners and all the other stuff. And it is my understanding your port is now in the process of using some of these for detection coming in. Could you briefly give us some thoughts on that?

Ms. ROONEY. Yes, sir. We have actually two different sets of radiation detection being used in the Port of New York and New Jersey now. First, we have the customs deployed radiation portal monitors that are now at all of our truck exit gates so all of cargo in New York, New Jersey is being scanned for radiation accept for that. That is going out by rail.

Mr. ETHERIDGE. Coming in or going out?

Ms. ROONEY. Coming into the commerce of the United States. So all of our import cargo that is going out through our terminals into the U.S. We are not scanning our export cargo at all at this point. So that accounts for about 88 percent of all the cargo in the Port of New York. And New Jersey is scanned for radiation.

The second project that we have going on is through the Department of Homeland Security Science and Technology directorate with a countermeasure test bed. And reference was made earlier to radiation detection equipment that is capable of doing the spectrographic analysis initially as opposed to waiting for a handheld isotope identifier.

We are testing that second and third generation equipment at our New York container terminals in Howland Hook.

Mr. ETHERIDGE. Thank you.

Mr. Ervin, given the questions I have just raised to Mr. Gold regarding foreign ports, given your experience in last duty assignment, which foreign ports do you think DHS should focus on in terms of security?

Mr. ERVIN. Well, I basically agree with what Mr. Koch said, that one of the factors, one of the key factors that should be considered in assigning risk levels to cargo coming in is the history that we have with the country as to whether that country has ties to terrorism, whether corruption tends to be a factor in those countries.

Of course, any cargo that originates, frankly, from ports in the Middle East or South Asia, because that tends to be the center of radical Islam, which is our principal foe nowadays, should be cargo about which we are especially vigilant at a minimum.

As you are suggesting, cargo that emanates from countries that have nothing to do with radical terrorism but that nevertheless originate from countries that historically have had an undue, or if not undue then a rather high incidence of corruption likewise should be scrutinized.

And to be fair, I think that those are among the criteria in ATS today.

Mr. ETHERIDGE. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman KING. I have one question, if anybody else has some additional questions. In the bill, we talk about funding being—an increase in funding coming from dedicated customs fees. I have no particular position one way or the other as to where the money should come from, but assuming there was a problem in the Congress with the customs, how would you feel if a dollar amount was put per container? What would the reaction be in the industry? What impact would it have?

I have heard the number of $20 per container. I have no idea whether it is 15, 20, 25, 40. Just take a number. If it is $20 per container were assessed, what impact would that have on commerce?

Mr. KOCH. Thank you, Chairman King. I think before we talk about what user fees should be put into place, the trade issury puts billions of dollars into the maritime industry, whether it is customs duties or other user fees that are being used. I think before we can discuss a $20 user fee or any type of user fee, we need to look at the system that is in place and what exactly is this going to cost. We can't just generally say, well, a $20 user fee out there and that will cover it, because we don't know what the exact costs are going to be.

I have been to Hong Kong. I have seen the ICIS system. In talking to people who were running the ICIS system, they said $6 to scan those containers.

We have heard Commander Flynn say 20 and as high as 50. I think before we can talk about any kind of user fee, we really need to evaluate the system that is in place and determine what the actual cost is and whether or not we are already putting money into those systems.

Mr. Chairman, I think there is not a lot of trust in trust funds, and for example, on dredging where there is already a fee being collected going into a dedicated trust fund, that money isn't all used on dredging. It is used for other federal purposes. So there is some concern that we not get caught up in that.

If the ICIS project is implemented, those charges will be implemented by the foreign terminal operating company to recover the cost of their capital investment in that equipment. So that would be a private sector fee that would be assessed on the cargo to collect that. It wouldn't have to come through a government.

But the final way to answer our question, I think, is that the industry, when the issue is raised about an additional container fee is always curious about, "for what?" And part of the problem here has been to really nail down clearly what is it the money would be spent on.

So, for example, where there is some even disagreement within the industry on an expanded port security grant program. There are many people who really wonder, "Okay, what is that money being used for?" Terminal operators, carriers, shippers are all incurring a lot of costs today to comply with the new security reg, so if more money is needed, clarity really should be provided. What is that money going to go for, and is it really something that the federal government should be paying for by virtue of a few recovery mechanisms?

Chairman KING. Mr. Ervin, Ms. Rooney?

Mr. ERVIN. Mr. Chairman, I would be inclined to defer to the industry colleagues as to what the impact would be on the industry. That said, whatever the figure is, and my sense is, based on everything I have read and heard, that the $20 figure is likeliest to be the one that would be sufficient here.

And by the way, the "it" that we are talking about is a fee to finance the cost of screening 100 percent of cargo of radiation. I don't think there is any question about what the fee would be used for. I think there is no question?

Chairman KING. Screening or inspecting?

Mr. ERVIN. That kind of points out the issue, doesn't it? I mean inspecting. I mean inspecting. But I think the point is well taken that trust funds in the past have been misused. I would ensure in this instance if we were to go to such a system that the funds would be dedicated to this purpose. So that is what I would say about that.

Chairman KING. Beth?

Ms. ROONEY. I echo Mr. Koch's comments that we would really need to know what that fee would be going for and what additional benefits or services are we going to get for it. But more important than that, the Maritime Ministry already pays billions and billions of dollars' worth of fees to the federal government some of which go into trust funds and comes back to the Maritime Ministry, most of which does not come back to the Maritime Ministry. So I think we should look at first the fees of the Maritime Ministry is already paying to the federal government and allocating some of those to port security before we start collecting new fees, sir.

Chairman KING. Mr. Pascrell?

Mr. PASCRELL. Mr. Chairman, your question, I think, your questioning focuses the committee's attention on what is the federal government's responsibility. We had a debate about this when we talked about the airline industry, if you remember. And I know they are different industries. The Maritime Ministry is very different. But just exactly what is the government's role and responsibility—

Chairman KING. Would the gentlemen yield for just a moment?

Mr. PASCRELL. Yes.

Chairman KING. I am going to have to leave. I have a meeting with some—

Mr. PASCRELL. I will be done in—

Chairman KING. No, no. Actually, Chairman Lungren is going to take over.

I just want to thank the witnesses for their testimony. There is a meeting that I have to go to. Thank you very much. Your testimony has been especially illuminating, and I particularly have gotten a lot out of the back and forth. I think it has educated all of us.

And usually, it is just Mr. Pascrell who engages in these types of debates. To have a panel doing it even adds to the?thank you all very much.

Mr. PASCRELL. We would have had a humdinger if we had five panelists, combine the panels, Mr. Chairman. You get dialogue, you know. It is not bad in a democracy if we try it out once in a while.

Getting back to my point, this is a supply chain, and in that supply chain, there are a lot of second parties. Becomes very complex here. You are talking about exporters, freight forwarders, whatever they are called, customs brokers, inland transportation providers, port operators, and ocean carriers. It is a pretty complex situation. We are not just talking about—I am interested in—

Mr. Gold, let me ask you this question, just a curious question, you know. Once in awhile I get to thinking. What is coming out of China? I am interested, because I have a sense of urgency. You should tell me today maybe I shouldn't think of things this way, but we all take it seriously what we are doing if we don't take ourselves seriously, but we know what our responsibilities are. What is coming out of China? All of these containers that go all over to the second shift and then third shift and they are moved from this vessel to another vessel. Do the Chinese inspect everything that comes out of the manufacturing, the industry which provides much of the retail on our shelves in the United States of America? Do they check each of those boxes before they get into a container?

Mr. GOLD. Congressman, I do know that as the boxes travel through China, the different Customs administrative authorities within China do look at the containers as they are moving through the country. I couldn't tell you what the actual amount is or what they do with it, but I think we want to focus on everywhere in looking at the supply chain security from the factory all the way through to the store floor.

Mr. PASCRELL. The only reason why I ask that is so much comes out of China that winds up on our ports, and, you know, I would hate to think that when we are looking at the GAO report and when we are trying to zero in on what are the percentages within reason, we know what error is, that a greater proportion of that which is not inspected are scanned or screened may come from China. I would be concerned about that, wouldn't you, Mr. Gold?

Mr. GOLD. Yes, but I think, you know, we?first of all, I want to comment on a comment you made earlier with regards to our statement. We fully support the department's policy right now 100 percent screening of all the manifests information that they receive and following up on that of 100 percent screening of the high-risk containers that are determined by the Automated Targeting System.

And again, we do need to bolster that system, looking at additional information. And again, that gets back to the original part of this looking at the supply chain as a whole, whether it is China, Africa or elsewhere. We need to focus on everything that we do abroad.

Mr. PASCRELL. So what you are saying is simply we should increase or improve the state of the art in screening knowing quite well that we can't inspect?

Mr. GOLD. Yes. I think we need to focus both on the automated targeting system.

Mr. PASCRELL. You think that is satisfactory? You think that is acceptable to the American people? Is it acceptable to you.

Mr. GOLD. I think we need to do as much as we can with the resources we have available right now.

Mr. PASCRELL. The resources that we have available. We are obviously not even spending enough money in terms of inspectors, et cetera, et cetera. I mean, we are not putting into this. We are not making this a priority. And again, I don't sense urgency. Maybe you do. Do you sense urgency on our part?

Mr. GOLD. I think there is an urgency on our part as the industry. We are trying to do as much as we possibly can. We don't want anything more or less in the container than what we have ordered from the factory. That is why our members are doing as much as they can with their vendors abroad and all their business partners.

Mr. PASCRELL. And you think we are doing enough, the federal government?

Mr. GOLD. As we have outlined in our testimony, we think more needs to be done, whether it is the Automated Targeting System, whether it is with C–TPAT, whether it is with business continuity planning. We definitely think more needs to be done.

Mr. PASCRELL. If I might just include this. When you are talking about—Mr. Gold, when you are talking about more has to be done, that is a very nice statement, very lovely statement. I use it, you use it. When you are talking about more has to be done to prevent nuclear weapons from coming into this country, it puts them in a different perspective, doesn't it?

Mr. GOLD. I would agree. That is why again, we need to focus on improving the systems we have in place and continue to focus on technologies in the future.

Mr. PASCRELL. And we had a report which is a year old. And if we go through this report and look through the recommendations, brief recommendations, what do you think we conclude in the year that we had this report as to where we stand right now?

Mr. GOLD. I know that both Assistant Commissioner Ahern and Deputy Secretary Jackson have addressed what has been done in the year since our report has been concluded. I think Assistant Commissioner Ahern addressed last week with clarifying from the numbers, and Assistant Secretary Jackson addressed it this afternoon.

Mr. PASCRELL. Then I conclude from what you say I shouldn't feel so much a sense of urgency.

Thank you, Mr. Chairman.

Mr. LUNGREN. [Presiding.] I thank the gentlemen.

I am just going to ask a couple of questions. One is, I am no advocate for France, but France was suggested as being an ally, and in court, we would say that may?we may be assuming facts not in evidence.

But the suggestion with France or some other countries have not cooperated with us on the CSI program, France being France, what if they turned around and said, "We will cooperate with you as long as you do the same thing in your ports"? What would the impact be on us if we were required to do the same thing in our ports that we are asking them to do? Ask each of you to give a shot on that.

Mr. KOCH. Congressman, I think that is an excellent question, and sometimes we lose sight of the fact that reciprocity is something we need to think about. As Bethann testified to, for example, on radiation scanning, we do radiation scanning on what is coming into the country. We don't do anything on what is going out of the

country. If we had to do the same thing going out of the country, we wouldn't be prepared to do it anymore than most of the rest of the world is prepared to immediately do it.

So if you impose conditions on trade that are going to be so onerous that our trading partners can't comply, they will, in fact, reciprocate and put mirror-image-type restrictions up. We need to take steps that improve security that makes sense. We need to be working with our trading partners. But we have to be able to do what we expect others to do as well. And in many cases, we aren't there.

So, for example, on the question of the Chinese inspecting the products they are sending out of their country to the U.S., our government doesn't inspect the 7 million containers of cargo we export out either. So there is this question here. Trade is a very voluminous thing right now in this nation. We are going to be importing roughly 12 million containers of cargo this year. We are going to be exporting probably about 8 million containers of loaded cargo this year. That is over a billion and a half dollars' worth of goods each day going through out ports. So we have a constant balance of trying to make sure that we don't cripple trade at the same time we come up with more intelligence security regimes.

Mr. LUNGREN. Anybody else? Mr. Ervin?

Mr. ERVIN. I would like to. Sir, certainly, other countries, it seems to me, have the right to demand that we do the very same thing that we are demanding of them. If France were to turn around and insist that they have the right to make sure that any cargo from the United States bound for France likewise be inspected and wanted to have the right to install French inspectors here to make sure that that gets done, I would be entirely for it. It seems to me that is the logical implication of what we are asking other countries to do.

If we don't do that, what we are essentially saying then is that CSI is humerical. It is essentially saying that, "Well, you, foreign country, have to really participate in this program only if you choose to. And if you choose not to participate in the program, you will continue in it in a nominal way." It has absolutely no integrity whatsoever.

Mr. LUNGREN. What did we have before CSI?

Mr. ERVIN. We had nothing, but what I am saying is, with CSI, we are not having anything. If countries don't have to inspect cargo that we tell them should it be inspected because we believe it to be high risk?

Mr. LUNGREN. I just asked the panel this question in order as you are sitting there. Are we appreciably more secure with respect to our ports? And I am talking about what comes in to our ports. We could also talk about the port security itself, access to it. I am just talking about what comes in to the ports given the fact that the whole impetus of this bill is, we are not where we need to be, and we need to do a lot more.

But have we had any appreciable gains in port security from the standpoint of cargo coming into the United States since 9/11?

Ms. Rooney?

Ms. ROONEY. In my opinion, we are appreciably better than we were and more secure than we were on 9/11. At the risk of giving Congressman Pascrell some ammunition, there is more that needs

to be done, sir. But it is all about creating a system of systems and a series of layered approaches. It has been said before that there is no single silver bullet. Not one of these programs is answer in and of itself. We can strength the existing programs that we have and develop additional programs, many of which are if your bill.

I personally think that if your bill goes forward with some of the changes that we have recommended in our testimony, we will be considerably more secure than we are today.

Mr. LUNGREN. Mr. Koch?

Mr. KOCH. I would agree. We have made significant progress and there is still more to do.

Mr. LUNGREN. Mr. Gold?

Mr. GOLD. I completely agree with both Chris and Bethann's statements.

Mr. LUNGREN. Mr. Ervin?

Mr. ERVIN. We have made some progress, Mr. Lungren, but we haven't nearly the progress that we should, and I guess the main point of my testimony is we haven't made the progress that we claim to have made. The programs upon which port maritime security are based actually do less than they claim to do for the safety and security of the American people.

Mr. LUNGREN. Do you think this bill wouldn't make a difference?

Mr. ERVIN. Yes, sir.

Mr. LUNGREN. No, but I mean a significant difference.

Mr. ERVIN. I think it would make a difference, and I suggested some further improvements in the bill. So I am a supporter of this bill.

Mr. LUNGREN. I thank all of our witnesses for your valuable testimony—you help us a great deal—and the members for their questions.

The members of the committee may have some additional questions for you, and I will ask that you respond in writing if we get those to you. The hearing record will be held open for 10 days.

We again thank the members of the committee and our witnesses.

And, without objection, the committee stands adjourned.

[Whereupon, at 5:20 p.m., the committee was adjourned.]

○