FOREIGN OPERATION OF U.S. PORT FACILITIES

(109–55)

HEARING

BEFORE THE

SUBCOMMITTEE ON
COAST GUARD AND MARITIME TRANSPORTATION

OF THE

COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 9, 2006

Printed for the use of the
Committee on Transportation and Infrastructure

U.S. GOVERNMENT PRINTING OFFICE

28–270 PDF WASHINGTON : 2006

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

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

DON YOUNG, Alaska, *Chairman*

THOMAS E. PETRI, Wisconsin, *Vice-Chair*
SHERWOOD L. BOEHLERT, New York
HOWARD COBLE, North Carolina
JOHN J. DUNCAN, JR., Tennessee
WAYNE T. GILCHREST, Maryland
JOHN L. MICA, Florida
PETER HOEKSTRA, Michigan
VERNON J. EHLERS, Michigan
SPENCER BACHUS, Alabama
STEVEN C. LATOURETTE, Ohio
SUE W. KELLY, New York
RICHARD H. BAKER, Louisiana
ROBERT W. NEY, Ohio
FRANK A. LOBIONDO, New Jersey
JERRY MORAN, Kansas
GARY G. MILLER, California
ROBIN HAYES, North Carolina
ROB SIMMONS, Connecticut
HENRY E. BROWN, JR., South Carolina
TIMOTHY V. JOHNSON, Illinois
TODD RUSSELL PLATTS, Pennsylvania
SAM GRAVES, Missouri
MARK R. KENNEDY, Minnesota
BILL SHUSTER, Pennsylvania
JOHN BOOZMAN, Arkansas
JIM GERLACH, Pennsylvania
MARIO DIAZ-BALART, Florida
JON C. PORTER, Nevada
TOM OSBORNE, Nebraska
KENNY MARCHANT, Texas
MICHAEL E. SODREL, Indiana
CHARLES W. DENT, Pennsylvania
TED POE, Texas
DAVID G. REICHERT, Washington
CONNIE MACK, Florida
JOHN R. 'RANDY' KUHL, JR., New York
LUIS G. FORTUÑO, Puerto Rico
LYNN A. WESTMORELAND, Georgia
CHARLES W. BOUSTANY, JR., Louisiana
JEAN SCHMIDT, Ohio

JAMES L. OBERSTAR, Minnesota
NICK J. RAHALL, II, West Virginia
PETER A. DEFAZIO, Oregon
JERRY F. COSTELLO, Illinois
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
BOB FILNER, California
EDDIE BERNICE JOHNSON, Texas
GENE TAYLOR, Mississippi
JUANITA MILLENDER-MCDONALD, California
ELIJAH E. CUMMINGS, Maryland
EARL BLUMENAUER, Oregon
ELLEN O. TAUSCHER, California
BILL PASCRELL, JR., New Jersey
LEONARD L. BOSWELL, Iowa
TIM HOLDEN, Pennsylvania
BRIAN BAIRD, Washington
SHELLEY BERKLEY, Nevada
JIM MATHESON, Utah
MICHAEL M. HONDA, California
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
ANTHONY D. WEINER, New York
JULIA CARSON, Indiana
TIMOTHY H. BISHOP, New York
MICHAEL H. MICHAUD, Maine
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
BRIAN HIGGINS, New York
RUSS CARNAHAN, Missouri
ALLYSON Y. SCHWARTZ, Pennsylvania
JOHN T. SALAZAR, Colorado
JOHN BARROW, Georgia

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

FRANK A. LOBIONDO, New Jersey, Chairman

HOWARD COBLE, North Carolina
WAYNE T. GILCHREST, Maryland
PETER HOEKSTRA, Michigan
ROB SIMMONS, Connecticut
MARIO DIAZ-BALART, Florida
DAVID G. REICHERT, Washington, *Vice-Chair*
CONNIE MACK, Florida
LUIS G. FORTUÑO, Puerto Rico
CHARLES W. BOUSTANY, JR., Louisiana
DON YOUNG, Alaska
(Ex Officio)

BOB FILNER, California, Ranking Democrat
CORRINE BROWN, Florida
GENE TAYLOR, Mississippi
JUANITA MILLENDER-MCDONALD, California
MICHAEL M. HONDA, California
ANTHONY D. WEINER, New York
BRIAN HIGGINS, New York
BRIAN BAIRD, Washington
JAMES L. OBERSTAR, Minnesota
(Ex Officio)

CONTENTS

TESTIMONY

	Page
Ahern, Jay, Assistant Commissioner for Field Operations, Customs and Border Patrol	3
Baker, Stewart A., Assistant Secretary for Policy, U.S. Department of Homeland Security, accompanied by Rdml Craig E. Bone, Director, Inspections and Compliance Directorate, U.S. Coast Guard	3
Brown, Gary L., Union Security Liaison, International Longshore and Warehouse Union	38
Carafano, Dr. James Jay, Ph.D, Senior Research Fellow for Defense and Homeland Security, the Heritage Foundation	38
Flynn, Dr. Stephen E., Jeane J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations	38
Nagle, Kurt J., President, American Association of Port Authorities	38
Scavone, Robert, Executive Vice President, Strategic Planning & Development, P&O Ports North America, Inc.	38

PREPARED STATEMENTS SUBMITTED BY MEMBERS OF CONGRESS

Filner, Hon. Bob. of California	98
Johnson, Hon. Eddie Bernice, of Texas	109
Kennedy, Hon. Mark, of Minnesota	113
Oberstar, Hon. James L., of Minnesota	121
Young, Hon. Don, of Alaska	179

PREPARED STATEMENTS SUBMITTED BY WITNESSES

Baker, Stewart A	70
Brown, Gary L	84
Carafano, Dr. James Jay	91
Flynn, Dr. Stephen E	100
Nagle, Kurt J	114
Scavone, Robert	125

ADDITION TO THE RECORD

Yoshitani, Tay, Senior Policy Advisor, National Association of Waterfront Employees (NAWE), statement	183

FOREIGN OPERATION OF U.S. PORT FACILITIES

Thursday, March 9, 2006

HOUSE OF REPRESENTATIVES, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE, SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION, WASHINGTON, D.C.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2167, Rayburn House Office Building, Hon. Frank A. LoBiondo [chairman of the committee] presiding.

Mr. LOBIONDO. Good morning. The Subcommittee will come to order. Before starting, I would like to ask unanimous consent that members of the Committee who are not on the Coast Guard Subcommittee may participate in the hearing today. We want to open this up. Do we hear any objection to that?

[No response.]

Mr. LOBIONDO. I don't think so. OK.

We welcome members of the full Committee.

Mr. Filner and Mr. Oberstar are on their way. On both of our panels, we have folks who have critical schedules, and I know the most important part of this will be coming to the questions. We talked to Mr. Filner's office, and I am going to start with my opening statement and ask Mr. Filner and Mr. Oberstar and Mr. Young, if they are here, for their statements; ask the other members to please forego opening statements. We will get into the testimony of the panel members and then get right into questions.

So, without further ado, the Subcommittee is meeting this morning to review foreign operation of terminal facilities at U.S. ports and to review the Federal Government's process in implementing effective port security measures.

Given the high level of foreign operations at U.S. ports, the complete implementation of the Maritime Transportation Security Act is vital to protect our security without dampening the international trade that is the lynchpin of our economy.

I still remain very concerned and opposed to the pending transfer of operational control over several U.S. port facilities to Dubai Ports World. A number of us still have many questions about this proposed deal, and hope that the witnesses' testimony will be able to address these complex issues.

Specifically, I am interested in learning to what level was the Coast Guard, Customs, and Department of Homeland Security involved with the initial review of the proposed sale and what level of participation each will have in the more stringent second review.

Secondly, what are the concerns that were raised by the Coast Guard and the Department, and how were those concerns addressed?

Also, does the fact that DP World is a foreign state-owned entity affect the Coast Guard's ability to share sensitive information with security officers who, by nature of their employment, could be considered agents of a foreign government?

I believe that these questions clearly demonstrate that we need to do a great deal more, and we have to give very serious thought and investigation before this sale is approved.

Along with my opposition to this specific transaction, I am extremely concerned with the Administration's lack of progress in implementing the broader port security measures this Congress passed as part of the Maritime Transportation Security Act of 2002 and successive legislation. It is now more than three years after the passage of the Maritime Transportation Security Act, and I am very frustrated to hear that many of these programs have not been implemented and, in fact, on some of them we have no idea when they might be.

Under MTSA, the Department of Homeland Security is required to develop the Transportation Worker Identification Credentials, known as the TWIC program, that will issue biometrically embedded security cards to maritime workers that can be used interchangeably at any U.S. port. To this date, we have not progressed beyond the prototype stage for this critical program, and without any creditable explanation.

The Department has not developed a format for the card or the readers that will be used to restrict access to secure areas in our ports. They have not developed a procedure to carry out the background checks for individuals who are applying for the card, or for the statutorily required biometric information that will be required on this card.

I find it totally unacceptable that the Department has allowed this program to be delayed for this long, clearly not giving it any priority. The TWIC card will be one of the primary means of keeping unauthorized personnel out of our ports, and I hope that the witnesses will be able to take back with them the very strong message that we expect this program to be moving forward and that we are tired of the delays that have incurred.

Likewise, MTSA requires the Coast Guard to develop and implement a system to track vessels up to 2,000 nautical miles from shore that will complement the near-shore tracking capabilities under the Automatic Identification System. The Coast Guard has previously testified that they are working through the International Maritime Organization to develop the components of a global system, rather than implementing a long-range vessel tracking system domestically.

While I guess I understand and somewhat agree that we should work with our international partners to develop a standardized system, again, I am very concerned and very frustrated by the Administration's apparent decision to delay the implementation of this system here at home. Excuses and delays for critical maritime security measures such as the TWIC card and the tracking system are unacceptable.

Finally, the Department is required to establish a secure systems of transportation program. That is protecting our supply chain to establish standards and procedures to secure the maritime cargo supply chain from the point of loading to arrival in the U.S. And of all the things that we are doing, making sure that these containers are protected before they get here is one of the most important.

This program will include standards for screening of cargo in foreign ports, standards for locks and seals to maintain security while in transit, and procedures for the Federal Government to ensure and validate compliance with this program. It is imperative that we develop robust measures to assure that this and other maritime security programs are being complied with. And I do not understand why the Department has absolutely disregarded this statutory requirement.

Integrity of our containers is essential and crucial if we are able to affect any measure of maritime antiterrorism and port security. We have taken steps to enhance security at our ports, but I believe we must do much more. The proposed transfer of the port terminal facilities to a foreign state-owned entity only highlights the need for the Administration to fully implement the full extent of the maritime security programs required under the Maritime Transportation Security Act and other laws to work with Congress to develop any further requirements. The American people expect us to take the necessary actions to secure our ports, and this Subcommittee will continue to work with the entire Congress to develop legislation to enhance our maritime homeland security.

I thank the witnesses for appearing today.

OK, we will break from the witnesses' testimony when Mr. Filner and Mr. Oberstar come in to see if they still wish to make any opening statements, but I would first like now to welcome our first panel: Mr. Stewart Baker, Assistant Secretary for Policy for U.S. Department of Homeland Security, accompanied by Rear Admiral Craig E. Bone, who is the Director of Inspections and Compliance Directorate with the United States Coast Guard, and Mr. Jay Ahern, Assistant Commissioner of Field Operations for Customs and Border Patrol.

Mr. Baker, please proceed.

TESTIMONY OF STEWART A. BAKER, ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY; ACCOMPANIED BY RDML CRAIG E. BONE, DIRECTOR, INSPECTIONS AND COMPLIANCE DIRECTORATE, UNITED STATES COAST GUARD; AND JAY AHERN, ASSISTANT COMMISSIONER FOR FIELD OPERATIONS, CUSTOMS AND BORDER PATROL

Mr. BAKER. Thank you, Chairman LoBiondo and members of the Subcommittee and the Committee. I will be brief. You have our prepared testimony. I will not be discussing port security, which Admiral Bone will discuss, or cargo security, which Mr. Ahern will discuss.

What I thought I would do is simply address some of the questions about the CFIUS process that may have arisen in connection with this transaction.

First, as the Chairman asked, what was the involvement of Coast Guard and CBP and the Department of Homeland Security in the process? The short answer is that both Coast Guard and CBP were closely consulted about this transaction, and DHS, actually within the Department, took the lead in addressing some of the security concerns that we in fact had raised.

As a result of DHS's efforts, rather than simply approving this transaction, it was approved only with a letter of assurances from the company, from both companies. That letter of assurances had two principal safeguards. First, it took several programs that are voluntary for other companies and made them mandatory, a best security practices program called the Customs-Trade Partnership Against Terrorism.

For every other company that is a voluntary program; you enter it in order to get certain benefits in processing. For P&O, Ports North America, and for DPW, those programs are not voluntary, they are mandatory. That requires a lot of recordkeeping and a lot of specific best security practices across the board.

They also assured us that we could have access to any data about their U.S. operations without a subpoena, without a warrant, we simply have to give them a written request for that data. That will allow us, among other things, to do background to obtain a list of all their current employees and to do background checks, run them against security watch lists and the like. And we will be exercising that authority as soon as the letter takes effect.

So we do have substantial protections that were at the instance [sic] of DHS and run to the benefit of both CBP and the Coast Guard.

That is a very brief overview of the process. We will be glad to take questions. I do want to emphasize that we certainly agree that the focus on port security and the many measures that the Chairman mentioned are appropriate areas of concern. We will be glad to work with the members of the Subcommittee and the Committee with respect to how to improve port security, and we look forward to discussing those ideas in the course of this hearing.

Thank you.

Mr. LOBIONDO. OK, thank you, Mr. Baker.

Admiral Bone?

Admiral BONE. Good morning, Chairman LoBiondo, Congressman Filner, and distinguished members of the Committee. I am Rear Admiral Craig Bone, Director of Inspection and Compliance for the Coast Guard, with responsibility for maritime ports, vessels, facilities, both their safety and security operations.

As Assistant Secretary Baker stated, I will be responsible for the security portion of this hearing, and we have undertaken and completed numerous improvements in our port, vessel, and facility security since Congress enacted the Marine Transportation Security Act and IMO established the International Ship and Port Security Code, which parallels MTSA.

Key to our efforts has been the Federal interagency cooperation, coupled with the engagement of the maritime industry and State and local officials, as well as law enforcement agencies. This was accomplished not just at the national level and through the regulatory process, but also carried out in our daily operation through

establishment of area maritime security committees with full interagency maritime stakeholders and State and local agency involvement.

All U.S. 3200 MTSA facilities in over 11,000 U.S. flag commercial vessel security plans have been completed by the operators and reviewed satisfactorily by the Coast Guard. Annual compliance examinations are conducted, as well as unscheduled targeted vessel boardings of U.S. and foreign flag vessels. Sixteen hundred boardings since July 2004 have resulted in 143 major control actions, including, in some cases, actually expelling the vessel from the port or not allowing it to come to the U.S. at all.

Annual compliance examination and random assessments of port facilities have been conducted, with 700 violations and 44 major control actions taken since July 2004. Those 44 would either stop cargo operations or even shut down the facility.

We truly appreciate the Congressional support which has provided additional assets in the way of MSSTs, small boats and crews, armed helicopters, increased inspectors, escorts and sea marshals to protect high-risk vessels, command center improvements to integrate operations, AIS receivers, improved traffic management system, intelligence personnel, and many more.

We have also conducted national level exercise, as well as local area exercises to test our response capability to threats or to an actual incident occurring to make sure there is better coordination.

Now, as I have said that, we know that there is much more to do. Some examples include implementing home port, which is a web-based system to improve communications within the ports and the stakeholders within the maritime community and the law enforcement agencies. We are conducting studies on the use of barrier booms to improve high-risk vessels and critical infrastructure; developing a marine security response team deployable 24/7 as a counterterrorism capability.

We are working to improve screening technologies and training for our passenger screening at both ferry and large passenger facilities; expanding AIS and LRIT, as you mentioned, through IMO; and improving our maritime domain awareness, as well as continuing replacement of our deep water assets, our aircraft, our command centers and systems in order to support offshore operations so we don't wait until the threat arrives here, but we address it as far offshore as possible; and, finally, working with TSA to implement the TWIC card, which you mentioned, which is a critical element to port security in our environment.

And while much has been done, I don't want in any way for the members here to think that we are complacent or feel that we have closed the vulnerabilities in our ports and our waterways or our maritime commerce that it supports. We look forward to working within DHS and across all the Federal, State, and local agencies and with the members of Congress as we continue to pursue security in the maritime environment.

Thank you, sir.

Mr. LOBIONDO. Thank you, Admiral Bone.

Mr. Ahern?

Mr. AHERN. Yes. Good morning, Chairman and members of the Committee and the Subcommittee this morning. My name is Jay

Ahern, and I am the Assistant Commissioner for United States Customs and Border Protection, and my responsibility is for our field operations, to include our ports here within the United States.

It is important, I believe, today for us to have the opportunity to discuss what role that we are playing in not only the CFIUS process, but also in securing the United States, particularly at our ports of entry. I think it is also important to have this Committee and Subcommittee have a full understanding of what our roles and responsibilities are, and I hope to outline some of those for you with our layered defense and our mechanisms that we have in place for protecting containers coming into this Country.

Our priority mission within CBP is homeland security, and we don't take that lightly at all, and we believe we are America's front line at our ports of entry for protecting against the entry of terrorist, terrorist weapons, weapons of mass destruction or effect from coming into this Country. And certainly I think it is also important to realize that America's seaports, the trading system is a global one, and it is important to continue to understand that process.

And as we secure our seaports, we take that into consideration, and it is certainly a work in progress as we craft an efficient system for providing security that is necessary for that supply chain, but also making sure at the same time we don't stifle legitimate trade coming into this Country that our economy and the global economy so much counts on.

I will tell you also that I believe very strongly that our 322 ports of entry in the United States are far safer today than they were previous to 9/11. And I believe since 9/11 our Country, as well as our organization, has made great strides in protecting supply chain and promoting trade and travel into this Country, while, again, maintaining the vitality of our economy, but never once taking our eye off our security responsibility.

Our Government responsibility and our private sector partners have instituted unprecedented programs to secure our seaports and the cargo moving through those seaports, and I think it is important that I state that none of these programs existed previous to 9/11. Before 9/11, also, we had four different agencies responsible, in three different Departments of Government, for protecting our borders at ports of entry, and today we have one unified border agency for that responsibility under the creation of the Department of Homeland Security and Customs and Border Protection that responsibility rests within this Department and this organization.

After 9/11, Customs, now Customs and Border Protection, developed a layered defense to secure the movement of cargo and, particularly for this discussion, containerized cargo coming into this Country, again, beginning security of the supply chain as deeply as we can in that supply chain, taking our officers and our strategies overseas to employ a defense and depth strategy, not making our ports of entry here in the United States the first opportunity to intervene or interdict, but to focus on prevention and getting as deep as we can in the support chain.

The first part of that five interrelated strategies I would like to briefly talk about is the 24-hour rule in the Trade Act. It required advanced electronic information on 100 percent of the cargo coming to the United States. One hundred percent of the cargo is sent elec-

tronically under the Trade Act 24 hours prior to lading in a foreign environment to the National Targeting Center here in Northern Virginia. The National Targeting Center then deploys a risk-based system called the Automated Targeting System, which is based on intelligence information, as well as a rule-based algorithm set of rules to target containers for risk coming into this Country. So it is important to know that that did not exist prior to 9/11.

At the National Targeting Center, we have representatives from the Coast Guard linking to the Intelligence Coordination Center, as well as to the FBI, Immigration and Customs Enforcement, Joint Terrorism Task Force. Many other agencies have representatives at this Center as well.

The third component is the cutting technology, cutting-edge technology we have deployed as well. At our seaports and also overseas we are deploying radiation portal monitors and large x-ray systems to have the ability to look inside the containers and also scan for radiation. Before 9/11, there were no radiation portal monitors deployed in our Country; today we have 181 at seaports around the Country, and we continue to deploy in a very rapid pattern.

Those 181 radiation portal monitors have the ability to screen 37 percent of the 11 million containers that come into this Country as they are departing terminals and ports within this Country to enter into the commerce of the United States. By the end of this calendar year, we will have 65 percent of the containers, throughout continued deployment of the radiation portal monitors. That is a very key link and a key component of our strategy as we go forward.

A fourth initiative that is very critical in pushing our borders out is the container security initiative. Again, this did not exist before 9/11. Currently, we have 43 ports. And that has changed from testimony in the last week and the week before from 42, because just yesterday we opened up in the Port of Salalah, Oman. So we now have 43 ports, accounting for about 75 percent of the containers coming into this Country originate in ports where we have United States Customs or Border Protection officers working with host country counterparts using large-scale imaging technology, as well as radiation detection capabilities to look at those containers that have scored for risk that we receive 24 hours prior to lading. Again, we did not have officers overseas before 9/11. As we move forward through the rest of this year, we will be at 50 ports and account for about 85 percent of the cargo coming through those ports.

The fifth initiative is the Customs-Trade Partnership Against Terrorism, and as the Assistant Secretary mentioned, it is a key component, it is one of the things that we did put forward as one of the assurances process. Fifty-eight hundred certified members are part of this program. These are some of the largest importers in the United States that are joined in partnership. I believe it is one of the largest and most successful public and private sector partnerships since 9/11 working together to ensure supply chain security.

Together, when you take each one of these five components and aggregate them together, I believe there is a very good layered strategy that is in place. Certainly every one of those programs is under a path of continuous improvement, and our goal is to con-

tinue to do that. But when you aggregate these five initiatives together, I believe it provides a greater protection against the introduction of the threat of terrorist attacks in this Country through the maritime supply chain.

I will conclude there, Mr. Chairman, and look forward to taking any questions on any of the layered defenses I have spoken about.

Mr. LOBIONDO. Thank you, Mr. Ahern.

I am now going to thank the Ranking Member, Mr. Oberstar, for joining us and ask Mr. Oberstar for his opening thoughts.

Mr. OBERSTAR. Thank you very much, Mr. Chairman, for moving out so vigorously and so forthright manner on this legislation, and for your quick response on the aviation NPRM that involves a similar issue of national security with our commercial airlines and the civil reserve air fleet issues that are associated with a proposed regulation change that would subject our airlines to foreign ownership and endanger our national security with the commercial air lift that was critical to Gulf War I and Gulf War II, moving personnel and equipment to the front lines aboard U.S. carriers.

For the past four years, since we enacted the port security legislation from this Committee—and it was this Committee that was the driving force in the House-Senate conference on that legislation, we have been trying to get the rest of the Congress and the Administration to pay attention to port security. It has taken this Dubai ports issue, rather badly understood by the public and not so well presented by the news media, to mobilize the Country into an outrage over the proposed sale of terminals at critical U.S. ports to a foreign interest which apparently a great body of the American public do not trust.

I would separate the issue that is before us today, Mr. Chairman, into two parts: the ownership issue and the capital flows associated with it, and the underlying but more important, far more overshadowing, port security issue. The question of capital flows is one that we have to think about as we look to ways of financing our ports, and to understand that, you have to put it in some context, that 20 percent of the world trade tonnage comes to the United States. Ninety-five percent of non-land trade, that is, from Canada or from Mexico, 95 percent comes by ship into the United States. Seventy-five percent of the value comes by ship into the United States.

We have 95,000 miles of shore line, 361 U.S. ports. Eighty percent of our port terminals are operated by foreign companies. Ninety-eight percent of the cargo that we import or export goes on foreign flag vessels. And that is an issue that has been going in the wrong direction for the last 32 years, since I have served in Congress, despite all of our efforts to build a U.S. flag maritime fleet.

So now we have in the range of 13 million containers coming into the United States, and the question is, where should they be screened. Our Port Security Act had the basic principle of pushing the border out. The further you go out with that border, the more secure, the safer the United States is. While a witness just said that we are going to have radiation portal monitors soon checking 65 percent of cargo, once it is here, it is too late.

We need—and the point of the Port Security Act was to screen those containers and that cargo oversees, before it gets into our

zone, our 200 mile economic zone. And that is the really significant failure of the last four years, a failure to enforce and carry out the provisions of the law, the key five provisions.

Our port security grants, the Coast Guard said that we need $5.4 billion to address the security needs at home and abroad. Congress has appropriated $883 million; the Administration has invested $700 and some million. We are short by any yardstick of measurement.

Background checks. The law requires that the Department of Homeland Security set standards for background checks for persons who have access to the secure area of ports. No background checks are required; no standards set for background checks.

Foreign flag security plans. The Coast Guard went to the international negotiations two years ago and settled on a plan that stops the Coast Guard from hands-on investigation of, an assessment of the security plans in ports and of vessels and vessel owners, and satisfies itself with the overall scheme of the country that says we have a security plan; they look at the plans and say, OK, that is good enough for us. That is wrong. That is wrong. And we, in 2004, tried to set the record straight and give the Coast Guard greater authority to go into those plans.

Foreign port security plans. The law requires the Coast Guard to conduct foreign port assessments on screening of cargo, access controls, authorized personnel, security management of those ports. Those assessments have not been completed for our largest trading partners.

Container seals, fifth point of the Security Act. We, in the law, require Department of Homeland Security to establish standards and procedures to secure cargo and monitoring the security while in transit, including standards for tamper-resistant seals. None of that has been done.

If those provisions had been put in place, Mr. Chairman, they would have greatly mitigated the concerns and fears of some foreign country or foreign company taking over management of the terminals at major U.S. ports. It still raises the question of whether the security review under the Florio Act has been carried out property, and there has been a 45-day extension.

But the President said, my position hasn't changed. If there was any doubt in mind or the people in my Administration that our ports would be less secure and the American people endangered, this deal wouldn't go forward, he said. Well, he is giving another review. It seems he has made up his mind.

Well, we are going to, in this hearing, get to the bottom of some of those issues and questions, and I appreciate very much that you have called this hearing, and I expect that we will have a good, in-depth look at the issue. Thank you, Mr. Chairman.

Mr. LOBIONDO. I thank Mr. Oberstar for his leadership on these issues and, again, one of the things Mr. Oberstar referred to which is disturbing for a number of us is that this proposal comes on the heels of what we found out sort of through the back door in November, I guess, that for the first time in our history we are proposing to allow foreign ownership of U.S. airlines. And there are many of us who feel that any foreign ownership of critical infrastructure is wrong.

That having been said, Mr. Baker, can you tell us—we understand that Secretary Chertoff was not made aware of the review that as ongoing in this process. Is that your understanding, that he was not made aware?

Mr. BAKER. That is correct.

Mr. LOBIONDO. Can you tell us why not?

Mr. BAKER. Yes. This process is run at the policy level, ordinarily, by the Treasury Department. The Treasury Department has a set of escalating committees so that disputes can be resolved, as they ordinarily are in the interagency process. The usual process is that if a transaction can be agreed on at the assistant secretary or staff level, then it is not raised to higher levels for discussion by the deputy secretaries or the secretaries.

In this case, the transaction received considerable scrutiny at DHS, from my office, from the Coast Guard, from CBP, and from other offices. We decided that we wanted to get more assurances from the company than had been provided; we negotiated those assurances. When we got the assurances that we wanted, since we were the last of the agencies with questions and concerns about the transaction, we reported back to CFIUS that our concerns had been satisfied. The CFIUS process then determined it wasn't necessary for deputy secretaries or secretaries to meet on the transaction, and it went forward.

For DHS purposes, the buck stops with me. I decided that we had sufficient assurances and did not brief the deputy secretary or the Secretary because they were not going to be asked to opine on the transaction in the interagency process.

Mr. LOBIONDO. Well, that is somewhat troubling to a number of us. I want to use my additional time initially here to talk about the overall maritime security measures. We had a discussion last week, when you appeared before the Armed Services Committee, about the Transportation Worker Identification Card. After that hearing there was an ABC News report that indicated a major security breach at the ports of New York and New Jersey. They went on to talk about the two ports handling millions of tons of cargo, scores of cruise ships that pass through each year, and that truckers who transport much of the cargo are issued ID cards which give them access to all areas of the port.

And ABC News learned that the cards given to thousands of truckers by the Port Authority of New York and New Jersey were issued with virtually no background checks and that an investigation at these two ports found stunning gaps in security; that the DHS report which was obtained by ABC News shows that of the 9,000 truckers checked, nearly half had evidence of criminal records, more than 500 held bogus licenses, and that officials were unsure of who the real identities were of these people. The intelligence report found that truckers that were in the category of not being checked had been convicted of homicide, assault, weapons charges, sex offenses, arson, drug dealing, identity theft, and cargo theft, and that some of those involved were identified with a gang called MS–13, which has been described as one of the most dangerous gangs in the United States.

Now, my question is if this is going on at the second busiest cargo port in the United States, why and how can DHS explain

that we have not put into place the identification card system and as of last week you could not tell us when we might expect it? Can we know anything about where we are going with this project?

Mr. BAKER. Yes, sir. First, I am aware of the study, and, of course, that was done by—the responsibility for those cards and the background checks was the responsibility of the Port Authority of New York and New Jersey; they made the determination not to carry out the background checks for a variety of reasons, I am sure. It is a subject of considerable controversy what kinds of background checks and what kinds of criminal behavior ought to exclude people from working in the ports.

There are not a lot of former choir boys who sign up to be longshoremen and the longshoremen are concerned that irrelevant criminal behavior far in the past might be considered disqualifying. So there are some reasons on the other side of those background checks why the Port Authority might not have determined that certain crimes were disqualifying for entry into the port.

Nonetheless, we agree with your basic point, which is that we do need to do background checks on the people who have access to our ports. That is why we have decided that, with respect to this transaction, we will exercise our authority under the assurances letter to gain access to the names of all the persons who work for the terminals that are being acquired so that we can do background checks on all of them.

More broadly, you have asked about the Transportation Worker Identification Card, and I have taken back the concerns that you raised at the last hearing in quite urgent terms, and I think it is fair to say that the Department understands the urgency of beginning this process. We finished the pilots last year, about the middle of the year, and I think in August received an evaluation of it.

We have been planning on what we will do to roll out a Transportation Worker Identification Card. Those efforts have been substantially accelerated and I think that we will be making an announcement within a matter of weeks to get that program up and running.

Mr. LOBIONDO. I certainly hope that is the case, Mr. Baker. We have such a high degree of frustration in not knowing how we can convey any more strongly than we have the unacceptability of the delays, and all the rhetoric doesn't account for anything. It has been pointed out over and over again if we have a terrorist incident at one of our ports, it is likely to shut down all of them. And all of these measures, including the Secure Systems Transportation program, securing the supply chain, which Mr. Flynn has been so eloquent about explaining. We have got to do something before these containers get here.

Unless the Department takes the cue from Congress with the laws that we pass and put some emphasis on this, we will be here a year, two, three years from now talking about the same thing, of why there were delays. I can't say it strongly enough.

Mr. BAKER. I fully appreciate the concern here, and we share it. I will defer to Mr. Ahern with respect to the details of some of the cargo programs, but we certainly don't believe that we are anywhere close to done with improving the security of the supply chain or the ports.

Mr. LOBIONDO. Mr. Filner.

Mr. FILNER. Thank you, Mr. Chairman. Thank you for holding the hearing.

Thank you for being here. I apologize for missing your opening statement, but from the tone of your answers, Mr. Baker, I don't see any sense from the Administration that you have changed your tone deafness on this issue, of the Dubai ports in specific or the port security in general. In answer to Chairman LoBiondo, you said, well, the buck stops with you, and Chertoff didn't hear this and the President didn't hear this. I mean, there was no sense of any mistake made. Do you think you made any mistake or do you regret second-guessing? Would you do it differently this time around, the next time around?

Mr. BAKER. Absolutely I would.

Mr. FILNER. Well, thank you. It took a revolution from the Country to say something.

But I just don't understand the lack of seeming concern. The Administration says it is still backing this deal, the 45 days doesn't mean anything. In your opening statement you didn't say anything about that. The House Appropriations Committee, as you know, voted 62 to 2—I don't know if there is any vote on that committee like that on anything—to overturn the sale. Are you still going to recommend a veto of this when the Congress does pass to stop on this?

Mr. BAKER. There is a certain constraint given that we are in a 45-day period in which we are carrying out our deliberations, but I can assure you that this is a full review without preconceptions of how it will come out. We are conducting additional fact-gathering with respect to the security practices of Dubai Ports World, with respect to P&O Ports North America, with respect to the Port of Dubai. Other parts of the Government are looking very closely at the record of Dubai and the UAE with respect to proliferation and trade. So I think we are conducting without preconceptions a———

Mr. FILNER. I hope you will tell the President what your results were, because he seems to have a preconception. He has continually, since this supposed review started, said he still backs the original agreement, and Dubai, I think, this morning announced that if we retaliate in this way, they would keep ships out of American ports. And it just seems that your initial unconcern about it from the point of view of security is leading us into a bigger crisis.

Mr. BAKER. I would beg to differ with respect to the notion that we weren't concerned about security. The assurances that we received in this case were unprecedented. For the first time ever we asked for special assurances in the context of a transaction involving U.S. ports.

Mr. FILNER. But the record that this Administration has on port security, which this Committee has raised since 9/11, Mr. Oberstar outlined them to begin with. You have not implemented the MTSA, the Maritime Transit Security Act, I guess it is called, in almost any of its demands on you. For example, we don't have security standards for containers; we don't have a way—we are not scanning the containers before they get into the United States; we don't have background checks, as has just been noticed; we don't have

secure entry to the marine terminals; we don't have closed-circuit TVs. I mean, we have more closed-circuit TVs, but we don't know what is in those containers when we learn here. And on and on.

So we are not convinced that the concern was fully taken, because there is all this other evidence. This has just sort of brought to the surface the problems that this Administration has been having.

And I represent San Diego, California, as you know. We were told by your agency that we did not qualify as a threat in your UASI—I don't know how you pronounce it—the Urban Area Strategic Initiative grants. And when I pointed out to Secretary Chertoff or some of your staff that I don't know of any port in America that has three nuclear carriers, a dozen nuclear subs, we have a nuclear power plant right nearby, we have the biggest Navy base in the world, and we are not a threat. And the reason we are not a threat, according to your staff, is that the Department of Defense assets are invisible to our calculations when dealing with threats. That is, because the—that is what they said—because we have the Navy there, we are defended.

I mean, with that kind of reasoning, we are a sleepy fishing village in the eyes of the Department of Homeland Security. And with that kind of thinking and that kind of blindness, of course we are not convinced that you took this seriously with the Dubai thing, because you haven't taken anything else seriously.

If you can't take six nuclear reactors sitting in the harbor of San Diego as a serious potential threat to terrorists—and we know that two of the hijackers were casing us out for six months, very much openly there—then something is wrong with your Department. And I said I didn't know the President's nickname for Secretary Chertoff, but I would say he's doing a heck of a job, Chertie, for all this. And I say that to you, based on your answers here.

It doesn't seem you are taking all this stuff with any seriousness. And why isn't San Diego a threat because we are the biggest Navy base in the world? Why wouldn't that be a potential threat to the Department of Homeland Security?

Mr. BAKER. We actually certainly appreciate the leadership this Committee has shown on both sides of the aisle in addressing these security issues, so I———

Mr. FILNER. All right, we are not going to get an answer here. I will just move on, Mr. Chairman. I have used my time.

Mr. LOBIONDO. Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman.

Gentlemen, good to have you all with us. When I view the operation of a port, I see a four-legged stool: you have Customs and Borders, you have United States Coast Guard, you have the terminal operator, and the port authority. Am I reading that correctly? Do you all see the same stool that I see?

Now, I met with a group of our colleagues and business leaders about three years ago from Denmark, Norway, Finland, and America, and many expressed concern there that port security must be enforced to the letter. But they were concerned that perhaps some of this enforcement may result in compromising the free flow of commerce. Do you have any comment on that?

Admiral BONE. Congressman, there is always a tradeoff any time you decide you are going to provide prescriptive measures or checks and balances in a system, because you are going to take the time to review, screen, examine, stop the flow or delay the flow. So there is always that tradeoff.

And it is a matter of risk management always in that process, and making sure and finding ways to target that through intelligence. Not just through intelligence, but also through history of working with those entities or those organizational entities, as well as randomly we are able to do that.

Now, do you operate a system with zero risk? No. Do we live in a world of zero threat? No. And I think the challenge for us—and with the guidance of Congress—is identifying what is that acceptable level, what are those measures. And we usually work that through our regulatory process to help define that, and then we prescribe it and put it into place.

Mr. COBLE. I got you.

Now, Mr. Hayes and I represent a State that has two ports, Morehead City and Wilmington. But these ports do not reach the volume of ports in, say, New York, Miami, et cetera. Are ports such as Morehead City and Wilmington receiving adequate resources to address the threats that are there?

Admiral BONE. Again, from the Coast Guard's aspect, we put into place the resources that Congress has provided based on risk, and we best placed those in those ports, working, again, with State and local entities. This isn't—I would have added a couple more things on your stool legs, which would have included the State and local authority which provide security and assist us as well.

Mr. COBLE. Good point.

Admiral BONE. And also looking at the industry segment and their capabilities to provide security as well.

Mr. COBLE. Mr. Baker, I am by no means a financial planner, but I know we are trying to come to some sort of conclusion that will assuage any of the discomfort that some of us have about Dubai. Has anyone thought about the possibility of a passive ownership that would perhaps remove them from the day to day operation of moving cargo offloading cargo? Has that been raised to any threshold?

Mr. BAKER. That is certainly an approach that has been used in other CFIUS cases, usually in the context of defense contracts involving very sensitive technology, where it is important for every piece of information that the defense contractor is dealing with to be shielded from the foreign owner. So because we are carrying out this review without preconceptions, that is certainly one possibility that we are going to look at.

Mr. COBLE. Mr. Ahern, I have ignored you, but not intentionally. Do you want to weigh into this before my red light illuminates?

Mr. AHERN. I would like to make a couple of comments back to your question of the impact of security in the Port of Wilmington. By our assessment, Wilmington and Morehead City are considered one and the same port, and only 37,000 containers out of the 11.3 million that come into this Country come through those ports. So we appropriately deploy the resources and the technology there to meet that threat.

I would also like to go back to your other question, too, about taking into consideration the impact on global trade and movement of trade as we move forward with security measures, and I think it also addresses a couple of the points that were brought up by Congressman Filner and also Congressman Oberstar, challenging the Department to move quicker; and certainly we want to move quicker and we are.

But I think it also needs to be restated factually again that we have taken our efforts overseas; we have begun defense in depth. We did not have anybody overseas pre–9/11. Today, in 43 ports throughout the world we have United States Customs and Border Protection officers there doing the screening and doing the examinations with the host country counterparts of those containers that pose a risk.

And also to, again, factually restate, as far as the radiation portal monitors are the tail end of our layered process, as once they are clearing at a port in the United States and leaving to go into the commerce of the United States. That is not the first or the only opportunity we have for intervention, that is the last end. So that is the end of our multilayered systems as we go forward.

So I just wanted to restate those facts, sir, also.

Mr. COBLE. Thank you. I see my time has expired.

Thank you, Mr. Chairman. Thank you, gentlemen, for being with us.

Mr. LOBIONDO. OK, thank you, Mr. Coble.

It is greatly appreciated that members tried to be considerate of all the folks who are here that we try to accommodate with staying within the time line. We have been alerted that we expect the first vote of the day probably in about a half hour. It is expected to be one vote, and then we should be uninterrupted for a while.

With that, I will turn to Mr. Oberstar.

Mr. OBERSTAR. Thank you, Mr. Chairman.

The additional review that is underway has brought this response from Dubai Ports World. They jointly request CFIUS to conduct a full 45-day review: "DP World and P&O Ports of North America will abide by the outcome of the review, but nothing herein shall constitute a waiver of any rights of DP World or POPNA that have arisen from the original notification."

You are familiar with that, Mr. Baker?

Mr. BAKER. Yes, I am.

Mr. OBERSTAR. What is the meaning of the statement that they are not waiving their rights from the original notification? Does that original notification, after the 30-day review, give them the right to complete the deal, that is, go to closing?

Mr. BAKER. Our view is that they have submitted themselves to CFIUS review, that that gives us the authority, the President the authority to say this transaction will not go forward or this transaction will go forward only when certain conditions are met, and that they are in no different condition than anyone else who———

Mr. OBERSTAR. So their statement that this further review does not constitute a waiver of any of their rights, that is vitiated by the review?

Mr. BAKER. In our view, that does not prevent us from issuing whatever order we would like to issue.

Mr. OBERSTAR. And in the course of that 45-day review, they cannot go to—they cannot close the deals themselves, cannot state that the original notification constitutes an authority to close?

Mr. BAKER. The Exxon-Florio Act doesn't distinguish between closed deals and open deals. The transaction is subject to review, and if the deal has closed, then the President has the authority to order divestment; if it hasn't closed, he has the authority to prohibit———

Mr. OBERSTAR. You can give this Committee an ironclad assurance that notwithstanding the statement by Dubai Ports World, that if the further 45-day review concludes that this is a security threat, that that can be terminated or modified in some way to protect the security interests of the United States?

Mr. BAKER. That is our view, and we think we have the—it is our interpretation of the statute that will govern. This is America; anybody can sue over anything, so I can't guarantee you there wouldn't be a lawsuit over that.

Mr. OBERSTAR. But a $6.8 billion deal will stay on hold.

Mr. BAKER. Most of the deal, of course, has nothing to do with the U.S. ports; the U.S. ports are about 10 percent of this deal.

Mr. OBERSTAR. Or it could go to closing and you could order divestiture.

Mr. BAKER. That is correct.

Mr. OBERSTAR. All right.

On the Container Security Initiative, Mr. Ahern, that is managed by your agency, Customs and Border Patrol. The proposal is to establish a regime to ensure that all containers that pose a security potential will be identified and inspected at foreign ports. However, not all foreign governments allow our Customs and Border Patrol to see a scan that has been requested; you only get notification that the scan was completed. And if it has passed, they will tell you it has passed, but that is all. What are you going to do about that?

Mr. AHERN. Well, I think first off, that is not the case, with the exception of possibly one country, where we have some concerns with certain privacy and authorities within one particular country. But in most circumstances we have our officers there with the host country counterpart as the scans are being conducted, and it has to be done to our satisfaction or we will issue a do not laid order for that container not to be put on a vessel for the United States———

Mr. OBERSTAR. Can you list for us———

Mr. AHERN.—if it is not reached to our satisfaction.

Mr. OBERSTAR. Would you list for the Committee, in a separate document, those countries where you have such presence and such screening?

Mr. AHERN. The 43 countries we have?

Mr. OBERSTAR. Yes.

Mr. AHERN. I would be happy to produce all of them for the 43 countries we have.

Mr. OBERSTAR. In a review that I conducted of the principal points of export to the United States, that was certainly not the case. Less than 5 percent of containers coming to the United States are screened.

Mr. AHERN. Five percent of the universe of 11.3 million is actually scanned.

Mr. OBERSTAR. Yes.

Mr. AHERN. One hundred percent of the containers coming to the United States are reviewed for intelligence and informational concerns through our National Targeting Center to score them for risk. One hundred percent of those that pose a risk through our scoring gets examined. If it is in a location where we have our officers as part of the Container Security Initiative, that scanning is done, that scanning is done overseas.

Mr. OBERSTAR. Well, I want to see the document that you have. We have had difficulty getting accurate data.

Mr. AHERN. I have them right in front of me, sir.

Mr. OBERSTAR. and I would like to have that.

Mr. AHERN. OK, we would be happy to provide that.

Mr. OBERSTAR. Thank you.

Mr. LOBIONDO. Thank you, Mr. Oberstar.

Mr. Diaz-Balart?

Mr. DIAZ-BALART. Thank you, Mr. Chairman.

Let me just make sure I understood this, because there is now this additional review, this further review. Was that also done—are there other facilities that have the same type of arrangement with foreign companies like the one from Dubai now is trying to get?

Mr. BAKER. The generally accepted figure is that about 80 percent of U.S. terminals are owned by foreign companies. So there are lots of foreign companies and some foreign government-owned companies that own or lease terminals.

I should stress that it is not necessary to go through CFIUS to acquire or even to acquire a company to obtain those interests; a foreign company could come into a port authority anywhere in the United States and ask to sign a lease, and if they met the port authority's requirements, they could simply sign a lease; and that transaction would never been seen at the Federal level, at least as far as CFIUS is concerned, we wouldn't have the authority to———

Mr. DIAZ-BALART. And it has been like that historically, correct?

Mr. BAKER. That is correct.

Mr. DIAZ-BALART. Are there, for an example, does Communist China have that sort of arrangement on any of our ports?

Mr. BAKER. There is a company in, I believe, the Port of Long Beach that is affiliated with the Chinese communist government that has at least stevedoring arrangements. I am not sure that they have a terminal.

Mr. DIAZ-BALART. This would be the same Communist China that held a U.S. military plane hostage and that who executes its own civilians pretty much at will. Was there a second review done there? By the way, I am not saying there shouldn't be a second or third or fourth review. My question is why was that not done with an entity such as this group from Communist China or other governments or other such countries?

Mr. BAKER. My understanding is that those transactions were carried out before this Administration took office, and I don't have details on it based on my experience.

Mr. DIAZ-BALART. But as far as you know, this kind of review didn't take place, including with such an organization that has

close ties or may even be owned by the communist Chinese government, the same communist Chinese government that held a U.S. plane hostage. As far as you know, there is no review like this?

Mr. BAKER. This review is the first review in which we were—the Department of Homeland Security was a member of CFIUS, was in a position to raise concerns. We raised concerns and the agreements that we obtained here are without precedent. So these issues were not flagged prior to our becoming part of the CFIUS process.

Mr. DIAZ-BALART. Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Diaz-Balart.

Ms. Brown?

Ms. BROWN. Thank you, Mr. Chairman.

Mr. Baker, I have a question, and I need some understanding, the Committee and the Country. The law is very clear in plain language, it says that the Department of Homeland Security's rationale for deciding not to proceed with the mandatory investigation as required by the plain language in the statute that the President shall—it doesn't say may—shall make an investigation in any instance in which an entity controlled by a foreign government should seek to engage in any acquisition that shall affect the national security of the United States.

Mr. BAKER. The interpretation of that language, which is that if there is no agency that believes that national security is at risk in the transaction———

Ms. BROWN. Put a period right there. In December the Coast Guard—the Coast Guard expressed serious concerns about the deal. I have a letter that was sent. Now, is the Coast Guard a part of an agency in this Administration?

Mr. BAKER. It is, but I don't think the Coast Guard expressed those concerns to the Department. Those concerns—I believe you are talking about an excerpt taken somewhat out of context, saying that there were certain intelligence gaps with respect to that.

Ms. BROWN. Excuse me. What is an intelligence gap?

Mr. BAKER. There were certain things that the Coast Guard did not know when it put together that report. In that report, despite the lack of that information———

Ms. BROWN. Sir, maybe the Coast Guard knew something that Homeland Security didn't know.

Mr. BAKER. The Coast Guard concluded that this transaction could go forward, notwithstanding that memorandum, which—and that memorandum itself concluded that there was not a risk to the national security from the transaction.

Ms. BROWN. You know, I have never seen an Administration that had such a contempt for the Congress in my entire life. The Coast Guard estimated that we need $5.4 billion for facility security. What did the Administration request?

Mr. BAKER. The $5.4 billion———

Ms. BROWN. Yes, billion, with a b.

Mr. BAKER.—was an estimate of the costs that would be incurred by the private sector in carrying out the Maritime Transportation Security Act. Those costs were not intended to be appropriated, those costs were incurred by the private sector, and have been incurred. The Administration has requested approximately———

Ms. BROWN. Forty-six million.

Mr. BAKER. Three———

Ms. BROWN. For all port security.

Mr. BAKER.—$3.4 billion for port security, counting the———

Ms. BROWN. This year?

Mr. BAKER. Yes. If you add in the port security operations of the Coast Guard, the C-TPAT and Container Security Initiative and the port security and security grants, it is well over $3 billion.

Ms. BROWN. Sir, listen. Don't play with me. Now, I'm asking about———

Mr. BAKER. I am not going to do that.

Ms. BROWN.—port security grants.

Mr. BAKER. Port security grants———

Ms. BROWN. In fact, the Administration requests doing away with them. And in answer to Mr. Filner's question, we put language saying that we wanted those ports to have high consideration with military—with military—because I have 14 ports in Florida.

So we had to go back, because we weren't rated properly on the scale, when we have all of that military equipment coming in. We put language in there that they should get high consideration. But now you all have recommended that we do away with port security. And who is bearing the brunt of this is not the Federal Government, but it is local government and it is the State. The Federal Government is not pulling their weight on this.

Mr. BAKER. I think we have suggested that the programs be consolidated so that they can be used———

Ms. BROWN. Bull. Consolidated. That means that you are taking the money, doing something else with it. Consolidation, I know exactly what it means, and local government knows what it means. With no help from the Administration, Congress has provided $883 million for port security. However, that amount represents only 16 percent of the Coast Guard estimated need. Explain that to me.

Mr. BAKER. The Coast Guard estimated those costs would be incurred by the private sector to carry out the facility security requirements of the Act. Those costs have actually been incurred; that has been done. Those are private sector costs, they weren't expected that we were going to be paying for them.

Ms. BROWN. Those are private security.

Can the Coast Guard person respond?

Admiral BONE. Again, what he has stated is accurate. Whenever you put a regulation in place, you have to do an economic impact analysis. Part of that analysis, in other words, is the cost worth the risk investment. And in the case this is what we had to say, was this was going to—these would be the costs incurred not just by the industry, but also by the other enforcement agencies, State, local, and individuals that would be engaged in providing assistance to secure the facilities and the vessels. This was both for vessels and security around facilities. So it wasn't implied that while there is an understanding that Congress put together a grant program to try to assist them———

Ms. BROWN. It was my bill, so I know the intent.

Admiral BONE. Yes.

Ms. BROWN. I know the intent of the bill.

Admiral BONE. Yes. And I am not questioning the intent. I am just trying to make sure the framework of what the estimate was based on. And I believe—it appeared to me, from where I was sitting, that the bill was to assist them with those costs.

Ms. BROWN. I yield back the balance of my time.

Mr. LOBIONDO. Thank you, Ms. Brown.

Mr. Reichert?

Mr. REICHERT. Thank you, Mr. Chairman.

Just a question for the panels regarding Seattle/Tacoma port areas. We have some companies owned by Korea, Japan, and Sweden, and I understand that there may be, right now, a deal on the table, a discussion, negotiations occurring with the Chinese government. Are you aware of the Chinese government showing some interest in operating port facilities in the Tacoma port, the Seattle port?

Mr. BAKER. I am not. I believe that, if there is a change of control, that that would trigger a reconsideration of the facility security plan so that, if it happens, the Coast Guard will get an opportunity to review the security aspects of that.

Mr. REICHERT. Yes, sir.

Admiral BONE. The only—there is one facility that currently is Taiwanese that has operations which has a Taiwanese relationship. So there may be—you know, because of that already, that linkage already being there, it is possible that something like that could be underway.

Mr. REICHERT. Thank you.

We talked about this four-or five-legged stool. Who has the ultimate authority for a particular port, is it the captain of the port, for security?

Admiral BONE. Yes, to allow a vessel to come in for port operations within the port itself, any vessel, we can deny any vessel to come in; we can close any facility or restrict its operation; we can restrict any person from coming to a facility or going aboard a vessel; we can expel a vessel from the port; we can dictate operations and restrictions within the port and the way it is carried out and set requirements around operations if we believe there to be a security threat.

Mr. REICHERT. Does the captain of the port also have responsibility for training, security training?

Admiral BONE. For Coast Guard security training, but also for standards set, to establish standards for industry as well, other than that which might have been by other regulation or congressional regulation.

Mr. REICHERT. So the port facilities owned by foreign governments or foreign companies would come under the jurisdiction of the captain of the port as far as training?

Admiral BONE. Yes.

Mr. REICHERT. Are those facilities also responsible for hiring any security personnel?

Admiral BONE. Yes. They are responsible for both the training program under MTSA and under the regulations that were implemented, as well as identification of security personnel and the responsibilities in providing security.

Mr. REICHERT. Who does the background investigation on those security personnel hired by those foreign governments or foreign companies?

Admiral BONE. The background investigation at this time is subject to State and local background checks.

Mr. REICHERT. There is no Federal background investigation on these employees?

Admiral BONE. No, there isn't.

Mr. REICHERT. Who is responsible for the training of the longshoremen? Do they participate in security training?

Admiral BONE. Again, the facilities, normally. Where longshoremen are employed, it should be included as part of their plan. And I know in New York and New Jersey, by example, there is an organization that went about training them collectively because they operate between multiple facilities.

Mr. REICHERT. Thank you, Mr. Chairman. I yield the balance of my time.

Mr. LOBIONDO. Thank you, Mr. Reichert.

Mr. Taylor, are you prepared or do you need a minute?

Mr. TAYLOR. Thank you, Mr. Chairman.

Admiral, number one, I want to congratulate the Coast Guard on having the courage not to tout the company line. And I am sure somewhere somebody's career is probably grinding to a halt. But I want to let you know I appreciate the concerns that have been expressed on the part of the Coast Guard. And I think our democracy is best served when people do speak their minds, even if it is not what the folks in the White House and maybe even the folks in this building want to hear.

What troubles me—and I think you articulated it pretty well—is rather than a physical or even electronic search of the containers, it has been the Coast Guard's policy to more or less rely on an honor system, an honor system involving, in many instances, a foreign manufacturer, a foreign port, a foreign steamship, and then you add to that equation quite possibly now a foreign nation-held port on our end. So given all of that, you have already got three weak links in the chain. Why would it make sense to add a fourth weak link in that chain?

Admiral BONE. Well, first off, post–9/11, we have the infrastructure and the laws that we have with regard to utilization of ports, who can operate within them, et cetera, and MTSA provided certain authorities to execute within that. I don't see everything as a weak link.

In fact, I see much of industry as part of our strength in that they have made significant investments in order to provide security. They have significant investments in and by themselves in the manufacturers themselves to protect their cargos and not allow them to be compromised. So———

Mr. TAYLOR. If I may, Admiral.

Admiral BONE. Yes, sir.

Mr. TAYLOR. What percentage of these Chinese firms that we are counting on to tell us something is wrong would be state-owned?

Admiral BONE. I don't have that—I don't have the exact———

Mr. TAYLOR. Is it fair to say that some of them would be state-owned?

Admiral BONE. Government? Government owned or influenced? If they are Chinese, I would imagine so.

Mr. TAYLOR. And aren't we at opposite positions over the future of Taiwan with the Nation of China?

Admiral BONE. Yes. But we have also had areas where we agree.

Mr. TAYLOR. OK. But getting back to the Taiwan issue, which apparently is the biggest issue at the moment, so, again, we are counting on, I regret to say, a possible foe, not necessarily a definite foe, but a possible foe to tell us if something in that container could harm Americans.

Admiral BONE. I would have to defer to Customs on the container-specific issue, as they own the container cargo portion of the supply chain. But we work closely as they target containers for examination, and if we find there is a threat or we believe there to be a threat, we will intercept it offshore and it won't arrive at our ports, if it is believed to be a threat and we are able to vett it.

I guess what I am not—I don't want to leave an impression with any member of Congress or anyone else that if there is a viable threat in the supply chain, that we don't vett that out collectively with CBP, Coast Guard, and any other agency, including DOD, to assist us in removing that threat from the U.S. or not allowing it to come here. And it could be a container, it could be an individual, it could be some other cargo that is not in a container. We know that drugs and illegal immigrants come in every day and not in containers. I don't void myself of all the other potential threat vectors.

Mr. TAYLOR. I am just curious Admiral—and, again, it is to make my point on what I think is the weakness of your honor system—what is the Coast Guard's policy on drugs for your personnel?

Admiral BONE. There is zero tolerance.

Mr. TAYLOR. Do you count on your personnel to come forward and say I smoked a joint last weekend, or do you have random testing?

Admiral BONE. No, we have tests. And maybe, I am sorry, you might not have been in here earlier, but since July 2004 we have boarded 16,000 vessels and turned away 143 of those vessels or expelled them from the ports as a result of their inability to provide for the security that is necessary. We do—we provide protection and escorts around other vessels so that they can't be compromised and there couldn't be a small boat attack.

Are we doing everything? Are we examining every vessel that comes in? No. But we are using the best intelligence in the targeting system in order to address that threat, and we don't believe—I don't believe for a minute that a terrorist will say, hey, here I am coming, I have got a weapon, and I am going to bring it to the United States. We address and we evaluate threat and risk every single day on every movement, whether or not it is coming foreign or it is moving through our waters domestically, and decide how to address it.

Mr. TAYLOR. What percentage of the approximately 20 million container equivalents that came into the Country last year were inspected by the Coast Guard or Customs?

Mr. AHERN. I can tell you exactly of the 11.3 million containers that came into the Country from foreign, 569,250 of those contain-

ers were examined by United States Customs or Border Protection. That is the 5 percent figure that continues to be utilized.

But I think it is important again to go back to the various layers in the overall supply chain. We do begin overseas with getting manifest information 24 hours in advance. We then run that through a very rigorous intelligence system to determine which one of those pose for risk. We look at that body, that 100 percent body that has been scanned and scored for risk, then receives our attention upon arrival.

We need to take into consideration also, as far as whether the verification process—we like to call it the validation process—of those partners that we have under the Customs-Trade Partnership Against Terrorism. We have gone to the foreign locations, to the suppliers, vendors, manufacturers, to see what kind of security practices they have in place. So it is a trust, but it also is a verified process that we have in place under that particular undertaking of our layered strategy.

Mr. TAYLOR. Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you.

I would please ask and remind all the members we have a lot that want to ask questions, to try as best they can for the five minutes.

With that, we will go to Mr. Simmons.

Mr. SIMMONS. Thank you, Mr. Chairman. I will do my best to say within the limit.

Thank you, gentlemen, for coming in and testifying today. This is clearly an important issue. Many of us have ports in our districts; many others are concerned about the security implications of this proposal.

Secretary Baker, on page 8 of your testimony you refer to the role of terminal operators and you say there has been a lot of attention in recent weeks about the threats posed by terminal operators. Let me clarify what they do. They do not run ports. They certainly don't provide or oversee security for the entire port complex. That is the responsibility of the government and the local port authority, which is usually a government agency, terminal operators do not obtain a comprehensive window into the breadth and depth of security measures, et cetera.

I think I understand what you are saying, but when I refer to Coast Guard Regulations 33 C.F.R. Chapter 1, Section 105–265, it states: Security Measures for Handling Cargo. General. The facility owner or operator must ensure that security measures relating to cargo handling are implemented. As it goes on, MARSAC Level 1. At MARSAC Level 1, the facility owner or operator must ensure the implementation of security measures. MARSAC 2: the facility owner or operator must also ensure the implementation of additional security measures. MARSAC Level 3: the facility owner or operator must ensure the implementation of additional security measures.

The facility operator is listed in these regulations at every level of security, and so I don't understand. As I understand your testimony, facility operators or terminal operators have no responsibility for security, but under the Coast Guard regulations they have responsibilities at every level. How are we to understand who is re-

sponsible, what those responsibilities are, and how are we to understand why there shouldn't be concerned, security concerns about foreign facility operators when it appears, under the regulations, that they are charged with security responsibilities at every level?

Mr. BAKER. I certainly would not suggest that they have no responsibility for security. And I think if you read on page 9 we actually say that the Maritime Transportation Security Act requires each terminal operator, because they operate inside the port, to file a facilities security plan with the Coast Guard that specifically details their compliance with all of the security measures required by Federal law, including those enforced by the Coast Guard. So there was no effort to say there was no security responsibility on the part of a terminal operator.

I think it is fair to say that the early coverage of this issue, in particular the first week, suggested that somehow we were outsourcing security for eight major ports to a foreign company. That was never the case, but it was a mis-impression that we were seeking to combat. There is no doubt that everyone who has a facility inside a port has security obligations that are enforced by the Coast Guard.

Mr. SIMMONS. According to these regulations, the facility operator is charged with detailed responsibilities at every level for security. According to your testimony, they don't run ports, they don't provide or oversee security for the complex, they do not obtain a comprehensive window into the breadth and depth of security measures.

I just think that if there is confusion on this issue out there—and I would say that in my district there is not a lot of confusion—they don't want these facility operators to be engaged in any great detail with the security operation of the port. But the regulations say they are. And that is the crux of the problem. If I can't figure it out based on your testimony and based on the regulations, how can the American people figure it out? And I guess their feeling is, hey, enough already; this is a bad deal, vote no.

Admiral BONE. Congressman, maybe just to explain a little bit. Within the confines of the facility itself, again, within from basically the pier to their gates, where the trucks come in and out of or people enter, and the fences around it, that facility, that is the responsibility of that foreign operator to provide for the security—in other words, access control measures, not to let people through, not to let people have access to those cargo, in other words, not unrestricted access to those cargos and to vett people as they come through there and to protect that facility against an external threat which may be by an individual or some other entity.

Those different MARSAC levels are different threat levels, and they correspond then to protective measures. It may be increased patrols, it may be increased security around particularly restricted areas where high-risk cargos may be placed. But that is what that responsibility really entails. It is not—in any way do they know what the Coast Guard, Customs, or ICE, or other agencies, or even State and local police security operations are with regard to other protective measures, or even our oversight and review of their operations in the conduct of their responsibilities.

So I guess I don't want to leave kind of a misunderstanding of what port security is versus that facility security responsibilities of that owner. Hopefully that helps.

Mr. SIMMONS. Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you. We are going to go to Mr. Nadler for Mr. Nadler's five minutes, then we are going to break for the vote and then go for a short recess for the vote and then come back.

Mr. Nadler.

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

Mr. Ahern, I think you stated that in 43 foreign ports all high-risk containers are screened electronically. Is that what you said?

Mr. AHERN. When we score the risk on the containers overseas at the 43 ports———

Mr. NADLER. That is what you said.

Mr. AHERN.—the protocol is for those to be screened before lading.

Mr. NADLER. Yes. The answer is yes. Thank you. What percent of all containers in foreign ports are screened electronically?

Mr. AHERN. Electronically? A hundred percent.

Mr. NADLER. What percentage of all containers are screened by gamma ray technology and by radiation scanners?

Mr. AHERN. OK, that wasn't your first—you said electronically.

Mr. NADLER. Forget that.

Mr. AHERN. A hundred percent through our systems are.

Mr. NADLER. I just asked the second question.

Mr. AHERN. It would be 1 percent.

Mr. NADLER. One percent of all containers are screened in a way that would assure us that no nuclear materials are aboard.

Mr. AHERN. That is the correct number today, yes.

Mr. NADLER. One percent. And when are we going to get to 100 percent?

Mr. AHERN. As we continue to deploy additional resources and technology to these ports.

Mr. NADLER. I asked for a date.

Mr. AHERN. Specific time frame, I don't have that.

Mr. NADLER. Would it be within a year or two?

Mr. AHERN. As we move forward for the rest of this calendar year———

Mr. NADLER. You are not answering.

Mr. AHERN.—43 to 50 ports, and that will get us to 85 percent of the containers———

Mr. NADLER. No, no, no. That will get us to 85 percent of the risky containers, right?

Mr. AHERN. That will get us to 85 percent of the entire universe of containers.

Mr. NADLER. Eighty-five percent of the entire universe of containers will be screened by gamma ray and———

Mr. AHERN. No.

Mr. NADLER. That was my question.

Mr. AHERN. Well———

Mr. NADLER. Please answer my question.

Mr. AHERN. Give me an opportunity to provide it in a full context.

Mr. NADLER. I am not asking for that. You provided it before. You are saying basically that eventually it will get to 85 percent—we will have this equipment in 85 percent of foreign ports and we will screen a lot of the containers that we determine are high-risk.

Mr. AHERN. That is correct.

Mr. NADLER. OK. My point is that I think it is absurd the same Department that determined that the Dubai deal is not high-risk determines which containers are high-risk. I feel very secure with that.

I believe that since any low-risk container from a reliable supplier on the way from the factory to the port somebody can substitute an atomic bomb for a television set, there is no such thing as a low-risk container. This Country will not be safe until every container is scanned by gamma ray and other technology to make sure there are no nuclear materials aboard.

Am I correct in assuming that there is no plan within a specific time frame by this Administration to put into place a situation which every single container is scanned in the way that I was talking about?

Mr. AHERN. That would be your understanding within our organization.

Mr. NADLER. That every—OK, there is no plan to scan every container.

Let me ask you a different question. Has the DHS mandated the use of tamper-proof seals on containers once they are scanned?

Mr. AHERN. We currently, in testing with container security devices and advanced container security devices, the initial results, we are only seeing about a 94 percent accuracy rate, which means 6 percent of that universe of 11 million containers need to be resolved because of false alarms or nuisance alarms. So we need to get———

Mr. NADLER. So right now there is zero percent using these tamper-proof seals?

Mr. AHERN. We are in testing with the sum number of those containers. Until we actually get a reliable———

Mr. NADLER. Ninety-four percent isn't reliable enough as an improvement over zero percent?

Mr. AHERN. Well, it means we will have to be resolving nuisance alarms or false positive-

Mr. NADLER. And it is better to risk atomic bombs in American ports than to resolve nuisance alarms?

Mr. AHERN. Of over 600,000 containers that are just nuisance or false alarms. That is not a good utilization of our resources, sir.

Mr. NADLER. OK. Now, not all foreign governments allow CBP personnel to see the scans, sometimes they only report the results of the scan to CBP, is that correct?

Mr. AHERN. That is correct in———

Mr. NADLER. And what do we do to those foreign governments to get them to change that policy?

Mr. AHERN. We are continuing to engage to go ahead and change that policy———

Mr. NADLER. We are talking to them, in other words.

Mr. AHERN.—to see if we are able to go ahead and actually have the images remoted to us. We are looking at that technology cur-

rently. And also please understand, too, that we have the ability to issue a do not lade order if it is not resolved to our risk prior to putting on board———

Mr. NADLER. Well, are we prepared to issue a do not load order to every single container that we don't see the scan of? And if not, why not?

Mr. AHERN. If that makes sense to us, that is what we will do.

Mr. NADLER. Excuse me. I asked you a question.

Mr. AHERN. That would not be———

Mr. NADLER. Are we prepared to do that now? Not if that makes sense. Does that make sense?

Mr. AHERN. We do it now when our risk is not resolved prior to lading.

Mr. NADLER. Well, but you are estimating a risk. I asked a different question. Does it make sense, and if not, why not, to insist on a do not load order on every container if we haven't seen the scan? And if not, why not?

Mr. AHERN. If the risk is not resolved to our satisfaction before it is placed on a vessel, it will be———

Mr. NADLER. Why should we not———

Mr. AHERN.—do not load order.

Mr. NADLER. Excuse me. Why should we not insist that we see every single scan? Why does that not increase our security?

Mr. AHERN. We are in the process of doing that right now with the remaining country we have had some challenges with. But we are getting———

Mr. NADLER. You just told me we are not doing that. We are not prepared to order a do not load order on every container that we don't see the scan of. You just said that.

Mr. AHERN. Let me put it in full context again, please. If the risk is not resolved prior to being put on board a vessel, we will give a do not lade order.

Mr. NADLER. Is there any other—all right. You are saying if the risk is not resolved, but that is somebody's estimate of the risk. On the assumption that every container has a risk if we haven't seen the scan, what are we doing and when we will be assured that we will see every single scan? Not every single scan of a container that someone decides is a risky container, every single container.

Mr. AHERN. I don't agree with your assumption. I think there needs to be risk management employed on———

Mr. NADLER. OK, so you don't agree with the assumption that we should inspect or scan and see the scan of every single container, only those containers that, on the basis of some outside parameters, are judged to be high-risk.

Mr. AHERN. No. What I want to state is, as accurately as I can, responsive to your question, is not every container poses a risk. You have a different view of that.

Mr. NADLER. Yes, I do. Now, why do some containers not pose a risk, because they are reliable suppliers? Why?

Mr. AHERN. Verification of the supply chain, suppliers, vendors, manufacturers, that have had———

Mr. NADLER. All right, but once you verify the supply chain, you have got a reliable supplier, et cetera, how can you guarantee that some driver wasn't bribed to take a long lunch hour and somebody

walked in, especially when you don't have tamper-proof seals that communicate with the U.S. Government on that container? How do you know someone didn't put something in that container, didn't replace a television set with an atomic bomb? So how can you always be certain of that?

Mr. AHERN. You can never be 100 percent certain.

Mr. NADLER. Ah. So there is always some risk.

Mr. AHERN. We assume a certain level of risk.

Mr. NADLER. We assume a certain level of risk and we are not willing to follow a policy to zero out risk on potential atomic weapons. That is what you are telling me.

Mr. AHERN. No, I wouldn't say that.

Mr. NADLER. You are saying minimizing the risk, but you are not saying zero it out.

Mr. AHERN. I am saying we accept a certain level of risk———

Mr. LOBIONDO. Excuse me one minute. I apologize for interrupting. We are just about at the six minute mark, Mr. Nadler.

Mr. NADLER. Well, just finish that answer.

Mr. LOBIONDO. You are well over five minutes.

Mr. NADLER. OK, I will conclude by summarizing, then, that you want to minimize the risk, but you don't think it feasible or proper or desirable to eliminate the risk, and we disagree on that. Thank you very much.

Mr. AHERN. I don't think it is feasible to scan every container coming into the United States overseas.

Mr. NADLER. Why not?

Mr. AHERN. I don't believe, first, there is a risk present to do 100 percent———

Mr. NADLER. You just said it isn't feasible. Why is it not feasible if we wanted to? If we spent enough money, why is it not feasible?

Mr. AHERN. Well, I think certainly if there are no limitations to finances, then certainly anything is possible.

Mr. NADLER. Would it cost billions or hundreds of millions or millions?

Mr. LOBIONDO. Let me apologize once again. Some of us don't want to miss the vote. I apologize to the panel. We will be in a short recess. We will be back as soon as the vote is over.

[Recess.]

Mr. LOBIONDO. We are going to reconvene. If our panelists would please take a seat.

Mr. Boustany was going to be next, but he is not here, so we are going to go with Mr. DeFazio.

Mr. DEFAZIO. Thank you, Mr. Chairman. I am in a simultaneous markup on aviation security. I appreciate the latitude.

I would like to go to the issue of the containers, Mr. Ahern. When I had to leave to go to the other markup, you had mentioned that if a container is identified by intelligence as a risk, it will be screened overseas if we have persons available. Is that correct? And then I understand subsequently you said 1 percent is screened overseas, but another 4 percent are screened here. So that means a total of 5 percent of all containers are identified as being at-risk, is that correct?

Mr. AHERN. Five percent of the universe is identified for risk.

Mr. DEFAZIO. OK. Now, let me see if I understand the system. There will be a factory somewhere, someplace where they load the container. We have inspected some portion of these workplaces to see that they have a paper plan and they have a security guard, or whatever else. But we don't have an ongoing presence at any of the places where these containers are packed, is that correct?

Mr. AHERN. We have done validations———

Mr. DEFAZIO. Yes, you have visited the site once at some point in time and said, OK. OK, so there is no American presence when it is packed. So then we receive an electronic transmission or bill of lading for that container which purports to tell us what is in the container. And then we crank that into our security universe and decide whether it is a risk. So we are not there when it is packed.

Now, when the container comes to the port, 1 percent are screened overseas, OK. Now, I understand there was also a discussion of the seals while I was gone, and you have 94 percent confidence that the seals are good enough, but that doesn't get into the whole idea of removing an entire panel of the container to access the contents and going around to the seal, does it? I mean, basically these containers can be opened without disturbing the seal, and even then, if you disturb the seal, you may be able to fudge that, is that correct?

Mr. AHERN. The full answer that was provided on the 94 percent figure I would like to restate for you.

Mr. DEFAZIO. OK, well———

Mr. AHERN. We are currently in testing———

Mr. DEFAZIO. The answer would be yes. OK.

Mr. AHERN. We are currently in testing and we have a 94 percent accuracy rate of the containers that are currently in testing, meaning we have 6 percent———

Mr. DEFAZIO. Again, any and all entry, not just the seal.

Mr. AHERN. The 6 percent false alarm rate on the current container security devices that are being tested.

Mr. DEFAZIO. But even that false alarm rate doesn't go to whether the container was entered somewhere else.

Mr. AHERN. These are container security devices. We are testing actually four or five different———

Mr. DEFAZIO. OK, that is good. Well, hopefully we can move ahead and we are not, you know, going to delay further.

Mr. AHERN. We would———

Mr. DEFAZIO. So now we have a container—excuse me, sir. So we have a container, we didn't observe it being packed; we have examined what they have told us is in it; 1 percent of the time we validate that; and then we have seals that can fail. Now we will get to the Admiral.

Admiral, we then load these things on ships, is that correct? And these ships, do we know who own ships registered in Liberia? Can we see through the registry now?

Admiral BONE. We do have the owner and the operator information, as well as the flag state.

Mr. DEFAZIO. Well, do we have it really or do we get back to a lawyer somewhere?

Admiral BONE. Well, if you are asking do we know the banking transitional, you know, and every layer behind it?

Mr. DEFAZIO. Right.

Admiral BONE. No.

Mr. DEFAZIO. OK.

Admiral BONE. We have someone, an entity that is legally liable and responsible.

Mr. DEFAZIO. But that doesn't tell us who really owns it, whether Osama bin Laden owns a fleet of ships or not, we don't know. Now, how about———

Admiral BONE. Well———

Mr. DEFAZIO. If we could, let us go to the crews, and we got into this a few years ago. The IMO has certified schools in the Phillippines, it has never physically visited them, and they have been documented in new reports as selling certificates. Now, that is a problem, because you end up with incompetent people. But beyond that, can you tell me that background checks are being run on the crews of foreign ships coming here?

Admiral BONE. I can tell you that all the crews, every individual that comes here, runs through an intelligence background.

Mr. DEFAZIO. Right. With their fingerprints?

Admiral BONE. No, there is no biometric———

Mr. DEFAZIO. No. We use the name.

Admiral BONE. There is no———

Mr. DEFAZIO. The name that they gave in the Phillippines when they bought the phony certificates.

Admiral BONE. They have a passport or a travel document.

Mr. DEFAZIO. Sure. Right. Those can't be forged, though.

Admiral BONE. And we have that as well.

Mr. DEFAZIO. A Belgian passport, do we accept those?

Admiral BONE. We have people trained to basically find and identify those———

Mr. DEFAZIO. Right.

Admiral BONE.—and we have.

Mr. DEFAZIO. Sure. But—so we don't know who owns the ships, we don't know what is in the containers, and we don't know who the crews are.

Admiral BONE. We do know the crews, sir.

Mr. DEFAZIO. Well, you know the names of the crews; they aren't fingerprinted, we haven't run thorough background checks. They are flying under flags that can be—OK, let us give you that. Do we track the ship? Because they have to tell us where they have been. How do we know where they have really been? Do we track the ships? Do we require transponders on the ships?

Admiral BONE. There is AIS transponders———

Mr. DEFAZIO. No.

Admiral BONE.—but there is not long-range identification to where I can place you———

Mr. DEFAZIO. Right, 20 miles and it only covers a few ports. Is that correct?

Admiral BONE. Sir?

Mr. DEFAZIO. So we don't cover the entire coastline of the United States with that system

Admiral BONE. The AIS transponders are required on all the vessels, and the transponders are able to be received by aircraft as well as by Coast Guard vessels.

Mr. DEFAZIO. OK. But we don't track every ship within 20 miles of our shore.

Admiral BONE. We don't have a vessel tracking system———

Mr. DEFAZIO. Right.

Admiral BONE.—that you are referring to, but we have the ability.

Mr. DEFAZIO. We have the ability. That is good. I appreciate it. Hopefully we will actually use that ability. Now, there are maritime companies that actually track their ships beginning to end, because they are worried—so let us give you everything on the containers. That is great, 94 percent reliability.

What if the ship stops in the Straits of Malacca and loads a nuclear bomb? Do we have any way, other than our intelligence people might tell us about it if they know about it, but we are not tracking that ship, so we don't know that they made an unscheduled stop in the middle of the ocean in the Straits of Malacca, because we are not requiring known technology, technology that is used commercially, the United States of America isn't saying, you know, what, no ship is coming to the United States of America unless we know where that was at all times and we track it at all times, because we are concerned they might stop somewhere and put—do we inspect the hulls of the ships?

I mean, we are worried about containers, but what about something that gets loaded on the ship? We are not very good on containers; what about loading something on the ship?

Admiral BONE. Let me answer your first question about tracking. We would have to go into a classified environment if we are going to talk about all the mechanisms of tracking that we have access to.

Mr. DEFAZIO. So you are telling me———

Admiral BONE. We don't have a commercial tracking system———

Mr. DEFAZIO. Right.

Admiral BONE. —that we track all ships with.

Mr. DEFAZIO. So commercial companies can afford it and some of the better ones use it, or they are worried about piracy, but we don't require it.

Admiral BONE. Again, the Coast Guard does not have a commercial tracking capability———

Mr. DEFAZIO. Right.

Admiral BONE.—that the Coast Guard owns and operates, other than near-shore capability.

Mr. DEFAZIO. Right.

Admiral BONE. And even the long-range identification tracking will be run out of some international body, most likely, rather than just a U.S.-owned or Coast Guard-owned and operated that will allow us to track commercial vessels. In fact, we have a group right now at IMO looking at the technical requirements at COMSAR and expect a vote this May from the full committee at IMO on LRIT, which looks extremely favorable.

But we are working to get to where you are asking, but we are not there yet.

Mr. DEFAZIO. Right. But I guess the point is, after 9/11, the United States could demand these things. We are the people who

are buying all this junk from around the world and running a huge and growing trade deficit, and people want to ship things here; we are not shipping much out, so they couldn't put retaliatory demands on us that we couldn't meet.

So the idea would be why not, if it is commercially viable technology, begin to demand that? OK, so we don't know exactly what is in the containers, but we might screen them here. We don't know if the ship stops somewhere and they loaded. What are we doing routinely in terms of ship inspections, given the fact that maybe the bomb isn't in the container, maybe it has been loaded into the hull of the ship at sea? I am not talking about once it gets in the port, because once it gets in the port, we kind of have a problem if they decide to detonate.

Admiral BONE. At sea—in fact, at sea, there are at-sea boardings. As I said, there are 16,000 boardings———

Mr. DEFAZIO. Out of how many ships?

Admiral BONE. Out of 7500 foreign flag vessels that make approximately 7200 visits———

Mr. DEFAZIO. Right.

Admiral BONE.—in the U.S. a year.

Mr. DEFAZIO. So we do a quarter of them, basically, a little more, a little less.

Admiral BONE. But I think, again, and, again, you know, you are going to go back to the same issue of targeting based on historical information and based on intelligence that we basically target vessels for that, both with regard to their cargo, their owner, their operator, their background history, as well as that of the people onboard, as well as where the cargo—the cargo itself and who it may be bound for. Those are all determinations of which vessels are boarded.

Mr. DEFAZIO. OK, so———

Mr. LOBIONDO. Excuse me, Mr. DeFazio.

Mr. DEFAZIO. Thank you, Mr. Chairman. I have got to go back to Aviation. Thank you.

Mr. LOBIONDO. OK. Thank you.

Mr. Boustany.

Mr. BOUSTANY. Thank you, Mr. Chairman.

Last week I read the Coast Guard report pertaining to the DP World transaction which cited intelligence gaps that would make it difficult to determine the actual risk involved with this transaction, and the Coast Guard, in general terms, reported that these gaps included a potential for foreign influence on DP World, unknown backgrounds of DP World personnel and general questions about terminal security.

And it is my understanding that these were resolved before the CFIUS approval, but they were resolved merely by obtaining assurances, as you had stated, Mr. Baker, that DP World would, in the future, provide the Coast Guard with additional information about personnel at the terminals and that they would enroll in the Customs-Trade Partnership, where they are saying that they will tighten security in exchange for the privilege of foregoing certain container inspections and so forth.

Has any additional information surfaced that has been provided by DP World at this time, as of today? Either of you.

Mr. BAKER. Why don't I let the Coast Guard address the intelligence report that they generated, and we can also talk about additional information.

Mr. BOUSTANY. Thank you.

Admiral BONE. Again, just as you stated, you know, his was an internal assessment, as we are a member of DHS and we are a full partner actually in review of the CFIUS process. And you are correct in that the letter of assurance—this is one of those areas where you know what you know and what you don't know you don't know.

The letter of assurances will provide us access to that information, and, again, the contract portion hasn't been—at which point in time the Department can ask for those names of those individuals, employees and other members of DPW or P&O if P&O personnel are being kept on to have the background check conducted, et cetera. So we don't see anything that limits us not only to know that, but also know what other agreements or operational agreements they have with other entities.

We don't have that visibility anywhere else other than, as the Secretary indicated, you know, at certain military load-out facility areas where those similar type of agreements have been reached. So I don't see anything that is going to preclude us from obtaining that.

We also have 30 days before a facility is allowed to operate that they are required to amend their facility security plan, at which point in time, for example, these letter of assurances, we can require that information or any other information we believe necessary to provide for the security of that facility. That is an amendment process that is currently in our regulations that we carried out under MTSA. Now, we don't—that doesn't necessarily prescribe a full security plan review, but we can identify those areas of risk that we believe we need to address.

Mr. BOUSTANY. What action would you take, under this promise of assurances, what actions would you take if you don't get forthcoming information within this prescribed period?

Admiral BONE. We don't allow operations.

Mr. BOUSTANY. OK.

Admiral BONE. No vessel could go to the facility. You know, you can own something, but nobody can operate it.

Mr. BOUSTANY. Do you feel like some of the information you have requested is starting to flow at this time?

Admiral BONE. Again, I think that once the transaction process goes to some level of completion, I don't know that specifically, but as that gets completed, then I fully expect, and I know the Secretary and Secretary Baker's intent is to pursue that aggressively.

Mr. BAKER. We have talked to the company, indicated that we expect to receive the information, and they have been entirely cooperative. So as soon as we make the request, we expect to get the information. We have done, using the assurance letters already, baseline reviews with both the Coast Guard and CBP inspecting current operations of the P&O North America terminals and have gotten a substantial amount of information there. Also, I believethe Coast Guard is doing a foreign port inspection of Dubai in this 45-day period.

Admiral BONE. What I might offer is we have completed examination of the P&O ports that they are planning to acquire, and we found them to be and remain in compliance, and part of the reason for that was literally to be able to say—for DPW to be able to not say these were problems that existed currently at this facility, before we acquired it, these weren't problems that we brought on.

Our folks just returned from Dubai, visiting all the DPW ports in Dubai and conducting port security assessment compliance with ISPS and found them in compliance with ISPS and, in fact, in many areas exceeding what we have in the United States with regard to security measures.

Mr. BOUSTANY. And you are referring to all the ports owned not only by DP Ports, but P&O as well? The entire system that would be?

Admiral BONE. Well, the P&O ports that are being acquired by DPW or where even DPW stevedore operations take place.

Mr. BOUSTANY. Thank you.

My time has expired. Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you.

Mrs. Kelly.

Mrs. KELLY. Thank you very much, Mr. Chairman.

There has been a great deal of attention paid to the container security, and appropriately so, but too often it is forgotten that Dubai Port World would also operate the Manhattan cruise terminal, where tens of thousands of passengers get on and off of boats; they enter and leave the Country every year. We have seen that Al Qaeda operatives have targeted cruise lines. The Washington Post reported that just three weeks ago. The United States does not let foreign countries play any role in security at America's airports, so it is concerning that they may play a role in security at America's flagship passenger seaport.

Before you answer—Mr. Baker, this question is directed at you—I know that you are going to reiterate the Coast Guard is responsible for ship security and terminal operations will continue as before, but you and I both know that operating the Manhattan terminal would give Dubai Ports detailed information about sailing times, passenger lists and locations, destinations, crew names and addresses, and other vital information that can compromise the safety of the ship and its passengers after it leaves the dock. Tell me what specific safeguards, if any, the United States Government has demanded from Dubai Ports to prevent any of this information from being shared with the company and utilized in an adverse way.

Mr. BAKER. I think the assurances we have received to date address that to some degree. We have the ability to see any information about their U.S. operations. That would include if we were concerned that they were gathering or transmitting information about sailing times or people involved in cruise ship landings, we can———

Mrs. KELLY. Excuse me, Mr. Baker, but how do you know if they are gathering it? We are in an electronic world; there is no paper trail.

Mr. BAKER. We have authority to ask for electronic trails as well, and it is very difficult, in fact, to hide electronic trails, both in transmission and in the systems that you use.

Mrs. KELLY. What is their obligation to respond if you request? Is it merely a request or is there some penalty attached?

Mr. BAKER. They have committed to us that they will provide, without a subpoena, any information that we ask for about any aspect of their U.S. operations. And as I think you heard Admiral Bone say, we have all of the authority we need to make sure that, if they lose our trust, they are not going to be doing business in the United States.

Mrs. KELLY. Well, if they own the port, sir, it is hard to say that they can't do business in the United States. I am extremely concerned about the flow of information that could jeopardize our cruise terminal in Manhattan. It is an important piece of the economics of Manhattan.

I want to go to another question I have, because I have only a few minutes, and I know you are in a hurry because you need to leave also.

The Wall Street Journal recently reported that the UAE refused a request from the U.S. Government in 2003 to intercept a shipment of nuclear technology facilitated by a man who was later convicted by the United States for violating the weapons of mass destruction sanctions. Can you discuss how this may have been factored into the Government's view of the UAE and this specific port deal?

Mr. BAKER. I am aware of the allegation, and we have assured members of the Congress that that is going to be examined in the course of the 45-day review by the intelligence community and by the members of CFIUS. So we are looking at that closely. I am not sure whether it was looked at by the intelligence community in the first review, and I am not sure that the charge has been verified; it appeared on a Web site. I don't know whether it is accurate.

Mrs. KELLY. The charge against whom, sir? The man was found, he was found guilty in a U.S. court, as I understand it.

Mr. BAKER. I think the question of whether———

Mrs. KELLY. In 2003.

Mr. BAKER. I am sorry, I thought you were referring to a 2003 incident in which Dubai was alleged not to have cooperated in an investigation.

Mrs. KELLY. No, the man was—this instance I am talking about, a man was convicted by the United States of America for violating the WMD sanctions. And I want to know if this was factored in on the UAE with regard to this ports deal.

Mr. BAKER. We did examine, through the intelligence community, all of the proliferation and terrorism risks associated with Dubai, the owners of the company. We also took into account our own experience with the company, with both companies, and they have been entirely cooperative and professional in their dealings with us.

Mrs. KELLY. I would like to have you give us more information about this, if you could.

Mr. BAKER. I would be glad to.

Mrs. KELLY. I know you are in a hurry and I am out of time. But I would appreciate getting more information about both of my questions.

Mr. Chairman, I hope that is all right with you.

Mr. LOBIONDO. Yes, without objection.

Mrs. KELLY. Thank you.

Mr. BAKER. Thank you.

Mr. LOBIONDO. Thank you, Mrs. Kelly.

Mr. Poe.

Mr. POE. Thank you, Mr. Chairman.

I represent Southeast Texas. We border Louisiana, where Mr. Boustany represents those good people. Between us is a river. We are glad about that. It is the Sabine-Neches Riverway. And you travel all the way up the Sabine-Neches Riverway, you show up at the Port of Beaumont. The Port of Beaumont ships one-third of the military cargo that goes to Iraq and Afghanistan. We get it from Fort Polk and we get it from Fort Hood. One of the terminals and stevedore operations involved in this UAE deal is a terminal and a stevedore operation that happens to load that cargo to Iraq and Afghanistan.

Of course, the port is protected by the Coast Guard. And, Admiral, I want to tell you that the Coast Guard folks there do a tremendous job going up and down that Riverway in those rubber boats. About half the people on active duty are reservists from all over the United States. They do a good job. I wanted to let you know that.

But this whole thing concerns me about homeland security. My background as a judge trying outlaws for 22 years always makes me suspect of what I see going on.

And, Mr. Baker, if I understand your comments correctly, you say that the UAE government-owned corporation is going to employ the best securities practice. And the more I hear about the cooperation of the UAE, this government that happens to own a corporation in our Country, it sounds like we are turning over security to that country, we are outsourcing homeland security to a foreign government. And we can label it something else, but that is the way I see it and the way it comes across to me.

A couple of questions. In this CFIUS situation, how many proposals have been denied since 9/11?

Mr. BAKER. It is difficult to say that any have been denied. A number have been———

Mr. POE. Let me understand your question. Have any of them been denied?

Mr. BAKER. Formally, no. Several, I am sure———

Mr. POE. How many of them have been reviewed?

Mr. BAKER. We do about 65 or 70 a year, so approximately 450, I think.

Mr. POE. And they have all found to pass muster on security issues?

Mr. BAKER. No, that is not correct.

Mr. POE. But none of them have been denied.

Mr. BAKER. Well, in many cases people have withdrawn them because they did not believe that they would get approval.

Mr. POE. Because they didn't pass muster on security issues.

Mr. BAKER. That is right.

Mr. POE. All right.

We have heard that the Administration is responsible for homeland security and basically through Homeland Security Department, comments have been made that we are in charge of that, so you can ″trust us.″ I don't do "trust us." I want results and obvious security measures that are employed.

Let me ask you a hypothetical. You know, if the war on terror takes us to some other country that happens to be an ally with the UAE, and here we are shipping cargo from Texas to the war on terror all over the world, doesn't common sense say that might be a problem, giving that information to a government that happens to own a company in a port that ships cargo for the war on terror? Doesn't common sense say that that is a problem?

Mr. BAKER. Obviously, there is a lot of information that you wouldn't want to provide to anyone outside the U.S. Government, and we do our best, as does the Defense Department———

Mr. POE. Let us just talk about the information they have. They have the stevedore operation, they have the manifest, they know when ships are leaving, they know what is on the ship, they know where the ship is going, they know who loaded the ship, they know when the ships are coming into port, they know where they come from and what is on those ships. That doesn't seem like maybe a security risk, letting a country, a foreign country have that information?

Mr. BAKER. Depends on the information. The information about what is coming in is not necessarily—what is in those containers is not necessarily known but to the terminal operator or to the stevedoring operation. They know what container they are supposed to move, they don't———

Mr. POE. So you don't see, in my hypothetical—I am sorry, I just have a couple of minutes.

Mr. BAKER. I am sorry.

Mr. POE. That hypothetical, you don't see that being a problem?

Mr. BAKER. There is risk in every transaction, and I am not trying to say that there is no risk in———

Mr. POE. Then why would we want to take another risk?

Mr. BAKER. This risk we believe we have taken special steps to minimize well beyond the steps that have been taken in the context of all the other foreign owners and operators of terminals in the United States today.

Mr. POE. It just seems like, to me, that this U.S. port marriage to the UAE has all the semblances of a bad marriage starting out. You know, they say that a failed marriage starts out what a deal, then it is an ordeal, then it is no deal. And I think this ought to be a no deal before it becomes an ordeal, Mr. Baker.

And I want to thank all of you for your time for being here. I have some more questions, but I am going to turn them in in writing.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Poe.

We are kind of in a dilemma here because we have got more questions for the first panel, but, Mr Baker, you have an appointment you are late for. Mr. Flynn has a plane to catch. We des-

perately want to hear you. And the other second panel members also have challenging time lines. We thought we were doing a good thing by opening this up to the full Committee. I am having second thoughts about it.

But to the first panel, gentlemen, thank you very much. We will probably want to try to follow up on some things at a future date. But thank you.

And we will do a switch-out to the second panel.

I thank the second panel for joining us. We have Dr. Stephen Flynn, who is the Jeane J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations. We have got Mr. Kurt Nagle, who is President of American Association of Port Authorities; we have Dr. James Jay Carafano, Senior Research Fellow for Defense and Homeland Security at the Heritage Foundation; Mr. Robert Scavone, who is Executive Vice President of Strategic Planning and Development for P&O, Ports of North America; and Mr. Gary Brown, who is the Union Security Liaison for the International Longshore and Warehouse Union.

With your indulgence, gentlemen, I am going to ask that Dr. Flynn give his statement, and we will try to allow you, Dr. Flynn, to get on your plane.

And then, Mr. Carafano, we know you have a pretty important appointment this afternoon, and we will try to clear you out as well.

Dr. Flynn, please proceed.

TESTIMONY OF DR. STEPHEN E. FLYNN, JEANE J. KIRKPATRICK SENIOR FELLOW FOR NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS; KURT J. NAGLE, PRESIDENT, AMERICAN ASSOCIATION OF PORT AUTHORITIES; DR. JAMES JAY CARAFANO, PH.D, SENIOR RESEARCH FELLOW FOR DEFENSE AND HOMELAND SECURITY, THE HERITAGE FOUNDATION; ROBERT SCAVONE, EXECUTIVE VICE PRESIDENT, STRATEGIC PLANNING & DEVELOPMENT, P&O PORTS NORTH AMERICA, INC.; AND GARY L. BROWN, UNION SECURITY LIAISON, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

Mr. FLYNN. Thank you very much, Mr. Chairman. I am delighted to be back with you again to talk about this very sobering topic. This morning we are, of course, talking about the Federal Government's progress in implementing the maritime security measures as required by the Maritime Transportation Security Act of 2002, and I would also like to provide some of my recommendations on how to advance this critical agenda.

Certainly, the controversy surrounding the takeover of five American container terminals by Dubai Ports World has had the salutary benefit of engaging Washington and the American people in a national conversation on the state of port security. This is long overdue given the enormous national security and economic security stakes should the next catastrophic terrorist attack on U.S. soil involve the global maritime transportation system and America's waterfront. While it has too often been lonely work, Chairman LoBiondo, I commend you and your Committee for your leadership in advocating that our critical maritime infrastructure should not

be overlooked in our post–9/11 efforts to secure the American homeland.

This is my second opportunity to appear before this Committee. On August 25th, 2004, I provided testimony that I entitled "The Ongoing Neglect of Maritime Transportation Security." At that hearing, I said, "I believe maritime transportation is one of the Nation's most serious vulnerabilities, and we are simply not doing enough to respond to the terrorist threat to this critical sector."

Sadly, I have seen too little progress in the ensuing 18 months to modify that assessment. Based on my visits to a dozen major seaports within the United States and abroad since 9/11, my conclusion is that the security measures that are currently in place do not provide an effective deterrent for a determined terrorist organization intent on exploiting or targeting the maritime transportation system to strike at the United States.

At the Federal level, the primary frontline agencies—the Coast Guard and Customs and Border Protection—are just grossly underfunded for what has become essentially a brand new mission for them, a major mission for them on 9/11. On the local and State levels, the size of port authority police forces remains tiny, providing often only token police presence within most seaports. While the Maritime Transportation Security Act of 2002 represented a constructive stepping off point for advancing security within this sector, we have made little meaningful progress since that passage of that Act.

In my remarks today, I will speak to both the shortfalls of our port security efforts within the United States and with our efforts to advance port security overseas and provide some recommendations on how to proceed. Our domestic and international efforts must be complementary because seaports, at the end of the day, are simply on-ramps and off-ramps into a global transportation network. To focus on just the security of U.S. seaports is a bit like hiring a network security manager who only puts in place firewalls to the computers in reach of his desk. If the whole network is not secure, such an effort would be futile.

To begin with, we must be candid in acknowledging that the MTSA is more of a sketch than a security blueprint. That is, it sets forth general requirements without establishing minimum standards for satisfying those requirements. For instance, the MTSA requires vessels and marine facilities have a plan for establishing and maintaining physical security, passenger and cargo security, and personnel security.

However, it does not actually define what that security is. It requires that there be a system for establishing and controlling access to secure areas of vessels or a facility, but it doesn't elaborate how that should be done. It mandates that there should be procedural security policies, but provides no guidance on what those policies should be.

The MTSA requires that there be a "qualified individual" to implement security issues, but sets no standards on what it takes to be "qualified." There are not even any minimal training standards that are required. The Coast Guard has worked with the Maritime Administration to create a "model" training course, but there is no

requirement that a facility or ship security officers attend a certified course based on that model curriculum.

The International Maritime Organization's International Ship and Port Facility Security Code, the ISPS Code, mirrors the MTSA in that it provides a framework of requirements without stipulating specific standards for satisfying those requirements. Ships and port facilities must have security plans, security officers, and certain security equipment, but the Code leaves it up to each foreign government to provide the specifics.

There are no minimum training standards for becoming a "qualified" security officer. There are no mandatory guidelines of what constitutes perimeter security. There are no mandated requirements to govern facility access controls. It is also important to point out that while most ships are in the business of moving cargo, the ISPS Code does not address cargo security.

When it comes to port security, the buck is essentially stopped outside of Washington, D.C. Since seaports in the United States are locally run operations where port authorities typically play the role of landlord, issuing long-term leases to private companies, it falls largely to those companies to provide for the security of the property they lease.

Just how far we have to go I think is best illustrated by the case of the Port of Los Angeles, our Nation's biggest port complex with Long Beach. In the case of Los Angeles, they have 7500 acres of facilities that run along 49 miles of waterfront, and that security is being provided by minimum-wage private security guards and a tiny port police force of under 100 officers.

The situation in Long Beach is even worse, with only 12 full-time police officers assigned to its 3,000 acres of facilities and a small cadre of private guards provided by the port authority and its tenants. I saw more security guards on the La Guardia security check on my way down here today than we have to patrol the entire Port of Long Beach. The problem of how to control what comes into the terminal is compounded by the fact that there are 11,000 independent truck operators who are authorized access to the port terminals, and yet there is no credentialing system in place to confirm the background of the drivers.

Mr. Chairman, you mentioned about the ABC report. At least in the case of New York-New Jersey, they actually have a pass system for who comes into the port. In L.A.-Long Beach, and most of our ports, that doesn't exist. So it would be difficult for DHS to go in and do these background checks of whether people have criminal records or not, simply because there is no pass system in place in most of our seaports.

The West Coast terminal operators have no way of even identifying who is on their facilities at any given moment. In the four years since September 11th, the two cities have received less than $40 million in Federal grants to improve the port's physical security measures. That amount is equivalent to what American taxpayers spend in a single day on domestic airport security.

Now, all this is on the on-ramp side of things, or the off-ramp here in the U.S. The real challenge is that we are facing a threat that is likely to emanate beyond our shores. And here the problems that I worry about are—I have talked to you about frequently be-

fore this Committee and others—is focused on the issues of the intermodel container, because it goes way into a country where we initially put into a factor, load it on local trucks that bring it often to multiple weigh stations before it gets to a major port, and then is loaded on a major ship arriving in the United States.

There are a lot of places along that trail where there is chance for real mischief. And we know there is because we have seen lots of crime and smuggling in the same system here. And, yet, when we look at the safeguards that we have in place to deal with all this, in addition to the limits of what is happening on the ports themselves, the challenge of physical security, perimeter security, access control and so forth, and when we face another piece of this will be the ships coming to us, we would like to know where they are—and, again, we have this Automated Identification System set by the MTSA, and yet the Coast Guard basically has a line-of-sight system where it does not have the means to routinely track vessels from long distances away. It is an honor system.

The 96-hour rule that requires that vessels tell us their last five border calls, that tell us what cargo they are bringing, that tell us who is on the ship is an honor system. There is no way to verify they are 96 hours out. There is no way to verify those are the five last ports of call they make. You can do a lot of detective work, but it is an honor system. The Coast Guard isn't routinely out there verifying that the vessels are where they say they are. And for most shipping, since it is legitimate, that works fine. But it is a problem worrying about the illegitimate that we need to be focused on.

The customs, of course, overseas is relying on Container Security Initiative teams. This is a big progress, putting agents overseas. However, their targeting over there is the same targeting criteria they use here, which is ultimately based on reliance on the cargo manifest information. This manifest information may not even provide the point of origin where the container was first stuffed. That would be an import document.

But that is not routinely provided to Customs 24 hours in advance of loading. So the decision about what poses a risk is based on essentially second-party information provided to ocean carriers who basically tell Customs this is what we think our customer says is onboard, and from there we decide what poses a risk or not.

The issue, of course, going back to the supply chain, relying on C-TPAT. This is a very positive thing involving the private sector in this enterprise, but because Customs does not have adequate resources to actually even process the applications, never mind routinely verify that in fact companies are living up to the security plans they provide them—and this is a complicated business—we have a lot of free-riders in this system, people who participate in the program that, frankly, are not vesting much in security.

We have, of course, the ISPS Code. We are required by MTSA, as requires the Coast Guard confirm that in fact overseas ports and terminals are abiding by this agreement. And yet, the Coast Guard has a total of 13 international security liaison officers to service Europe, Africa, the Middle East, Latin America, and the Caribbean. Now, Brazil has 25 ports onto itself, but a country visit is

often a two-to three-day stop-by, visit one port, and the country is good to go.

What we are building here is a house of cards. What is going to happen when we have a maritime incident is virtually all these initiatives to manage risk are going to be implicated. It will be from a C-TPAT company, it will be going through a CSI port on an ISPS-compliant facility, on an ISPS-compliant vessel, and it will arrive in the United States and will have a major maritime terrorist incident.

And when we want to restart the system as we close down afterwards, we are not going to be able to restore public trust because the kind of questions that you are asking today are going to be asked with a lot more rigor post the next event. And if we can't answer satisfactorily that risk can be managed, we are going to shut down the system.

We are putting a lot of money into something called missile defense. The technology that is associated with that is a very high bar. The expense is quite high. But we are saying in that program, basically, a zero tolerance about the risk of weapons of mass destruction put on a ballistic missile sent to the United States. And, yet, we basically have a trust-but-don't-verify system for being able to safeguard us in the event that a weapon of mass destruction is put in a cargo container and shipped into our ports.

We have a very long way to go. The technology is there. I think the will and the capabilities within these agencies are largely there; they simply haven't been resourced, it has not been made a priority. And if we don't get this right, what we are seeing, I think, in these last few weeks is the kind of reaction that we would likely get post an event. This is like a World Trade Center I scenario we hear.

We are worried about the potential security risk associated with DB Ports World deal, and, in my own view, it ranks very near the bottom of the concerns to have the specific issue of terminal operators, because all these other gaps should be of much higher priority. But we are worried about it enough that we are looking at fundamentally changing the way this system works. And I worry that post the event that we may have in the not-distant future, we won't even have a conversation about how best to do this, we will just simply take actions that may in fact be cures worse than the disease.

Now is the time to act, to work out the kinks, to put into place a robust system. But what is key to remember here is that the terminal operators at the end of the day, the global terminal operators, like DP World, whether it ultimately gets this piece of properties on the U.S. or not is going to have to be a part of how we deal with global security, maritime security.

Dubai World is going to have one-half of the Port of Karachi. If you want to get a weapon of mass destruction from Pakistan to Dubai, or anywhere else in the Middle East, you are probably going to go through a container terminal. One-half of it is going to be by a global terminal operator called Hutchison Port Holdings, the other is going to be Dubai Port World. We are going to need to cooperate with that terminal operator to put in place counter-proliferation controls, even if something is not destined here.

So we have to be very careful, I think, as we proceed with our legitimate concerns about seaport security in the United States that we are keeping an eye on the fact that it is a global system, and we have to work with all the partners who are legitimate. If that is what the end of the 45-day review gives us, we have to work with them in order to put in place the adequate safeguards.

Thank you very much, Mr. Chairman.

Mr. LOBIONDO. Thank you, Dr. Flynn. We are going to ask a couple of questions of Dr. Flynn and let him try to catch his plane.

Thank you for this rather comprehensive overview of where the shortfalls are, and I know that you have been talking about this for years. And if there is any good to come out of this latest incident with the United Arab Emirates, it is that I think more attention is being paid to maritime domain awareness. Your testimony last week before Armed Services I think was very powerful. I have appreciated the fact that you have at least gotten the attention of more people with your ability to get the story out on 60 Minutes and National Public Radio, which I both listened to—I have listened to both.

But we have a great deal of frustration because most of the members are off doing other things, everybody is pretty busy, and this window that we have to make an imprint on changing how we are handling port security is, I think, very small. And I am very frustrated that we can't seem, no matter how loud we shout, no matter how loud you shout, to get other members of Congress, to get the Administration to pay attention to these issues.

Obviously, if we had an incident, people would pay attention very quickly. And, obviously, if we had an incident, the faucets of money would open up and, you know, money would flow into port security like it did the aviation security, some $25 billion overall.

With what you have seen, Dr. Flynn, and what you have heard and what you have observed, we have got the aspects of the MTSA, which have not been implemented, where no action has been taken, and there are lot of critical areas here. But the difficult part getting any of them started is then trying to prioritize, because they are not going to do them all at once. If you had to offer us advice on what we should focus the most on, the quickest, what would you say?

Mr. FLYNN. I think the first is the need to focus over there, to continue what has been an effort—certainly the Administration has taken important steps in putting Customs agents overseas and adopting the ISPS Code in order to get our trading partners and other maritime nations to share a common vision about where we need to go. The problem is there still isn't much behind these curtains.

And so I think the top priority should be working with the overseas terminal operators and putting in place a system that are being piloted in Hong Kong, where every container coming into the truck gate, or one of two truck gates and two terminals in the Port of Hong Kong—the busiest terminal in the world is the Hong Kong International Terminal—is getting a radiation image, a cargo scan image, and a picture of the container's number and putting it into a database.

The ability to capture all that data—not necessarily to examine and scrutinize everyone, but capture all that data—is something that I think the industry can put in. The technology is available, and it would help us in so many positive ways, both in terms of creating I think a more effective deterrent than what we have now in the system, but basically give a primary screen tool even to deal with false alarm issues that we don't have right now if we target a container overseas, which can wear out your welcome mat. For the 1 percent you have, if you constantly pull boxes out and it turns out there is nothing there, you are causing disruption, you are causing expense, and so primary screens of everything coming through could be helpful.

It also can support counter-proliferation. I was talking about that in my remarks the Karachi to Dubai issue. The Department of Homeland Security doesn't have that as a focus, but the President has made counter-proliferation a top priority. Well, this material, as we know from Kahn network, moves through this system. As we build visibility in the system, we provide the means to support counter-proliferation as well. And I would hope that some resources come out of the intelligence community could then be applied to this problem, not just relying solely on Customs and Coast Guard's resources to deal with this.

So putting this basically—turning to the terminal operators, the four biggest in the world would account for about 8 out of every 10 boxes coming to the United States, encouraging them to essentially make this investment, which they can recover through a surcharge for imports coming through, would be a big step forward that I think many who have looked at it said this could work at a reasonable cost, without disruption, that would make it a qualitative leap forward and giving us physical evidence that low-risk is low-risk.

The second priority I would make would be the issue of some sort of third-party audit of the security plans. Customs will never have enough agents to do this; Coast Guard will never have enough agents to check everything overseas. Let us create essentially a third-party audit system where we then, Government, audit the auditors by setting high bars, bonded systems, folks that go out and check whether in fact companies are living up to what they say they are doing in terms of supply chain security.

And the third option in terms of priority would be getting a handle on the whole issue of who is in the port on our end, because you can attack a port not just by bringing stuff overseas, but just by driving a truck in it full of explosives, and there is plenty of that stuff around here as well. So the need to get on with the credentialing process and knowing who is in the port, the TWIC process plus, anybody who is in that port, we should know who they are in order so that we can, if we have intelligence, we can manage that, but we can have some sense of adult supervision in these critical assets.

So those would be the three things I would focus on: moving towards overseas, developing a radiation and gamma imaging and other technologies, creating database of what moves through the system, the third-party audit, and then, lastly, the TWIC process.

I just want to make, I think, an important point as well about radiation portals that are currently deployed a lot in our ports that

the Assistant Commissioner Ahern spoke about. Radiation portal technology such as the one we are using today will not help you find a nuclear weapon; they will not find—they won't be able to detect a nuclear weapon, they won't help be able to detect a lightly shielded dirty bomb, and they won't detect highly-enriched uranium.

Other than that, it is a great technology. It is capable of spotting plutonium and an unshielded dirty bomb. And the idea of putting radiation portals with gamma imaging together is that the radiation forces the need for shielding, and then the screening will see a dense object where there is not supposed to be a dense object. That application makes sense; it is affordable; it has been demonstrated in Hong Kong.

But running away with lots of radiation portals in the United States and doing ribbon-cuttings to say we have made ourselves safe from nuclear weapons here is not quite true with basically what—representing what that capability really provides. We really need to get a handle on that.

Mr. LOBIONDO. How long has the Hong Kong project been running?

Mr. FLYNN. It started first in one terminal, Modern Terminal, in September, the first sort of startup, but it really has been running full test since January 2005. So a full year now or 14 months. In that time they have collected more than 1.2 million images of everything moving into those gates. And if I put that in contrast, CBP, through the Container Security Initiative, has examined about 3500 containers during that year under the CSI protocol. So we are capturing and have the ability to capture that amount of information.

And this is no U.S. money and no Hong Kong government money; this is the terminal operator who invested in this capability, one who, by the way, does not have any terminals here in the United States. Hutchison Port Holdings has no terminals in the United States, but is vested in the network and vested in the system, and is terrified, legitimately, that if we shut it down, their whole enterprise implodes.

Again, I think it is important to realize these global terminal operators, with appropriate checks and supervision, are an ally in how we can go about building a system, they are not just the problem. The key is not the ownership, for me, it is adequate rules and oversight of those rules. And we have to partner with foreigners—it is part of dealing with that outside world—and we also have to make sure that they are playing by rules that safeguard our interests. And my experience has been, dealing with terminal operators, all of whom are foreign owned, and many of the liners, is that they are for leaning on this, because it is their billions of dollars of capital investment that are at stake.

Mr. LOBIONDO. My recollection from Armed Services last week, when you gave testimony on the Hong Kong pilot project, was that DHS indicated that maybe this could work, but we don't have anywhere near enough data and we have got to wait much longer to see if in fact this is viable. In your view, how much longer do we have to wait before we decide that this is a viable system?

Mr. FLYNN. Well, the good news is there is progress. DHS, the Deputy Secretary, Michael Jackson, has essentially directed the Department in late December, Customs, to take a solid look. They have begun the process. They have a sample, I believe, of 20,000 images, which are now sort of looking at how will they work into the protocol.

So it is not a case that they have not been entirely disengaged from this process; they have been tentative because it is not a sponsored project. There is no requirement for them to evaluate this or anything else. So they have been looking at it sort of hesitantly, but now there is more engagement on it, which I think is constructive.

The issues are legitimate on CBP's part. You know, they have legitimate concerns about essentially giving another big ticket highly visible program without their resources to actually manage it, the IT backbone, numbers of inspectors and personnel and so forth. Those are legitimate concerns. I mean, if the industry ends up making what could be about a $1.5 billion investment to do this globally in the four biggest terminal operators companies and we work to get that built in the rest of the area, and it turns out CBP doesn't have the IT trunk to access those images, doesn't have enough inspectors to do examinations, then it is an albatross for them.

And, so, given the track record of setting new requirements like the MTSA—I mean, the MTSA requires that the Coast Guard do all these audits, but nobody provided any new billets for them to do it; they had to take it out of hide. So there are legitimate concerns, I would say, within the bureaucracy about taking on another ambitious program, but not adequate funding to actually execute it and then ending up being with more egg on their face.

This is a soluble problem. We are not talking about massive numbers of people. The IT problem is manageable. The people in San Diego can, right now, see all those images that are being collected in real-time through—remotely in San Diego. So it can be done in Northern Virginia, where the National Targeting Center is, as well, as the actual containers are moving through, if they knew to target it.

But certainly they can go after the archive. It is doable, but there are practical issues. You need to have the IT backbone, you need the bodies. And if this is a big program, then they need the resources, they need commitment from the Administration and from this body, obviously, that they will get them.

Mr. LOBIONDO. I have got a couple more, but let me turn to Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chairman.

It is good to see you again, Dr. Flynn. Dr. Flynn, this morning's testimony—I don't know if you heard Mr. Ahern's testimony in response to my questions this morning. He said that it was not feasible to require scanning of all containers in the foreign port. Is there any reason it is not feasible?

Mr. FLYNN. I mean, I think in principle, yes, we could mandate it happen. What I would be worried about is right now there is not the technology available to deploy this in this next year. If we said

this applies by July 1st, everybody has to have it, it wouldn't be feasible———

Mr. NADLER. Because we don't have enough of the scanning machines?

Mr. FLYNN. Yes. The machines would have to be fabricated. Nobody has taken on that scale of a project, so you would have to manufacture them, you would have to deploy them———

Mr. NADLER. How long do you think it would take to do this?

Mr. FLYNN. I think you could set a clock, a reasonable clock, of two to three years, and———

Mr. NADLER. So we could require———

Mr. FLYNN.—graduated process.

Mr. NADLER. So we could require that in two to three years every container be scanned in the foreign port before it gets put on a ship bound for the United States?

Mr. FLYNN. I think that the marketplace could respond to that requirement if it were set with that kind of time frame. What I would say is that there is an opportunity I hear I think with this controversy that the main operators would do it on their own if they know that in fact the data they would produce is going to be used and if basically they can apply a surcharge to cover the costs.

Mr. NADLER. Now, Mr. Ahern also said that we don't need to do that, in effect, because we are on track, that we are going to be scanning all the high-risk containers. Now, it is my contention, and I sort of said this to him, that we don't really know what high-risk containers are, that our low-risk container, the driver can be bribed to take an extra long lunch hour and somebody can put an atomic bomb in a container operated by a very reputable company, and no one knows the difference.

So, in your judgment, is it necessary for the security of this Country to really go on track toward scanning all the containers, as opposed to somebody's judgment as to what high-risk containers are?

Mr. FLYNN. I think the good news with the application in Hong Kong is it is not possible to build it into the truck entry process without scanning every container, including those who don't come to the United States, that, basically, it doesn't make sense. You can't create a traffic pattern for just U.S.-bound containers. That means the cost of doing this is applied to everybody.

The issue becomes actually analyzing all those images, and the time that that would take. Now, clearly I think, in time, you are going to see computer-assisted tools that will so support that, but the answer—the particular concern I share that you have, Congressman, which is how is it that Customs knows what is high-risk. And the fact is, as we know, our intelligence services are broken big time, and we are having a real struggle reorganizing that, and I would say it is 10 to 15 years before we are probably going to———

Mr. NADLER. So we don't really know what is high-risk and what is low-risk.

Mr. FLYNN. We don't. And, further, the assumptions about what is risk is built around past efforts of criminality, which are ongoing conspiracies. And there we can see that there is a tendency to

gravitate to the weakest links in the system, but terror is actually likely to be a one-short deal———

Mr. NADLER. Exactly.

Mr. FLYNN.—and so penetrating a legitimate company once is doable in almost any circumstance.

Mr. NADLER. And, therefore, there is no definition of high-risk and low-risk that makes sense in an anti-terrorist situation.

Mr. FLYNN. Well, I think you have to view every container as a Trojan horse and as a high-risk.

Mr. NADLER. OK.

Mr. FLYNN. If we can verify it in the systems that we are talking about here would provide to mean that low-risk is low-risk.

Mr. NADLER. So we should go to a system where we require every container be scanned as rapidly as feasible.

Mr. FLYNN. I think we can go to that system, and it would be, again, setting a reasonable time frame so the market could respond.

Mr. NADLER. As rapidly as feasible.

Mr. FLYNN. And then—I do. And what I would set, though, is a tiered system for analysis right now———

Mr. NADLER. OK.

Mr. FLYNN.—that would basically use———

Mr. NADLER. Yes, you said that in your testimony.

Mr. FLYNN. Very good.

Mr. NADLER. Let me ask you a different question. Right now we don't require seals on the containers that are tamper-proof and that would notify, in effect, a GPS or somehow notify the United States if that container was tampered with or opened after it was scanned. Do you think it would be a good idea or a mandatory idea to require such seals on all containers after they were scanned?

Mr. FLYNN. Yes, I think we have certainly got to do something about the seal issue. Again, there are lots of ways one could defeat the technology. You would want to have it checked. I would say one thing about building this beachhead in an overseas terminal is if you did have the seal and it had that information, it could be downloaded before it enters the terminal. So that would work, I think, well.

Mr. NADLER. OK.

Mr. FLYNN. There are still some kinks with these seals; the false alarm issues and how you reconcile them and so forth. One thing is the Operation Safe Commerce Initiative, but nobody knows what the results are. You know, this has been treated as super-secret stuff. We need to know what basically we learned as a Government by doing lots of tests and figure out how we can improve on it. But I think we will reach a point where seals are used on containers for supply chain visibility and accountability purposes.

Mr. NADLER. Thank you. Finally, Congressman Oberstar, the Ranking Member of the full Committee, and I yesterday introduced the Sale Only If Scanned Act, the SOS Act, which essentially requires—the bill said one year; maybe we will change it to two years—that no container can be put on a ship bound for the United States unless that container has been scanned with the latest available technology as defined as you have been talking about—gamma radiation plus—gamma ray plus radiation detection—and

has a proper tamper-resistant seal that will tell you if it is tampered with; and that we should require as a matter of law that no container can be put on a ship bound for the United States until that has been done.

Now, within this time frame of two to three years, do you think that is reasonable legislation, that that would greatly enhance our security, or not?

Mr. FLYNN. The key is the time frame.

Mr. NADLER. Within the time frame that you specified.

Mr. FLYNN. My sort of approach here right now is let us see if we can get the four main terminal operators to jump forward and do it here and work out the kinks, and then definitely set the requirements that would move. We want a universal system that gets us there.

And I think there is an opportunity here for the terminal operators themselves to embrace this if they get the right signal from the U.S. Government that we would use the data and move forward. There is some value in that, obviously, if the market takes the ownership of the issue, but the signal from Congress that basically we need to have a trust-but-verified system and we need the best———

Mr. NADLER. And what we heard from the Administration this morning is that they see no necessity of scanning any but the high—as they define the high-risk containers. Your testimony is we don't really know what high-risk containers are because of a one-shot terrorist deal, and that we must go to a system where we will scan every container as soon as feasible.

Mr. FLYNN. I think if we adopt that globally, we will also make a big step forward on counter-proliferation, which is also another critical issue of our time.

Mr. NADLER. Yes. Thank you very much.

Mr. LOBIONDO. Just one last question, Dr. Flynn. Is Hong Kong able to do anything with chemical or biological scanning?

Mr. FLYNN. Let me be clear that what this pilot project that was done by the private company was designed to show if it was possible to collect scanning data on every container, truck entering into a busy terminal at 300 trucks an hour. No analysis was done on this data because the private players don't make judgment about the risk, it was they can make this available. So the answer is no on the chemical and biological, there are not sensors in place. It is a radiation portal, it is gamma ray technology. That is what it would be focused on.

Mr. LOBIONDO. So that would be a whole separate problem we would have to worry about.

Mr. FLYNN. It is a complicated problem, particularly when you get to biological. The problems with biology, most of the tests we use, like pregnancy tests, have very limited shelf life because they actually have live agents in it to react to the agent. Chemical is a little more straightforward.

But with the tools we have, I think you are able to do both the imaging I think is important to see whether you are seeing things in a shipment that is not supposed to be there. The notion is, if it evolves, as you merge commercial data, you will start to have archival information what Nike sneakers look like repeatedly, and

the software will automatically check and say there is a big something in here which doesn't belong; it could be a weapon, it could be components for a weapon of mass destruction, or it could be chemicals or whatever.

That would be helpful obviously for dealing with the counter-drug issue as well. A lot of the chemicals, for instance, that are used for methamphetamine are coming out of a place like India. Legitimate companies and transactions end up in Mexico. We can't see that right now, and that feeds that problem. The more transparency and visibility we can advance from the system, a lot of public goods will be served beyond just a terror threat.

Mr. LOBIONDO. Mr. DeFazio, Dr. Flynn was trying to catch a plane. I don't know, if you have got questions, if you will be able to———

Mr. DEFAZIO. I always—I have read his book. I appreciate his comments. Mr. Chairman, sorry, I have been back and forth with the Aviation Transportation Security Administration markup.

And I don't know if this would be repetitive, but, if you could, Dr. Flynn, I have seen your comments in the press regarding the Dubai transfer and where it doesn't raise to a level of concern, but you are raising other points about security at the ports. I don't know if you were here for the first panel.

Mr. FLYNN. I was, yes.

Mr. DEFAZIO. You know, I—I mean, do you think that some of those issues I raised, the fact that we really don't track ships as they move, I mean, something could feasibly be on-loaded, even if we had secure containers? And my understanding from the testimony is we don't have secure containers.

I mean, are you looking outward and sort of moving back into the U.S. in terms of your ideas? Because, I mean, the idea that we screen 1 percent of containers overseas and the rest here seems a problem, because, once it is here, they don't necessarily have to deliver it to a predesignated spot to cause mayhem.

Mr. FLYNN. I am, and I think all those scenarios are there. Again, the honor system we have in place right now for a very scary scenario, which is a bit crazy, I think. But certainly in terms of every ship crossing the Pacific and the Atlantic Ocean that is legitimate and is of a legitimate size is using MARSAC to communicate with their home office.

You can't talk to a satellite without giving away where you are. It would be possible to use existing technology of commercial networks here to track most of the ships moving across the ocean at a nominal cost. And why we are not there, why we are building a whole system to see line-of-sight—the Coast Guard is not out there patrolling every bit of the time around the clock.

Twenty miles at 20 knots is an hour in a very big ship. I don't think a plane will fall out of the sky when you shoot at it, you have got to stop something with a lot of momentum. And that is not going to happen if there is nobody there.

There was a sea marshal program, as you may recall, early after 9/11. The Coast Guard ran out of money, so it stopped doing it. So now it is relying on risk data and intelligence. Well, this is an area that we don't exactly have—it wasn't at the top of the intelligence food chain to monitor what was going on in the maritime transpor-

tation industry, so how we miraculously, after 9/11, had such good intelligence we could run a risk-based approach, without having any verifications in the system, I think is a bit of a stretch.

We need the best intelligence we can get, but we need verification on the way, and there is lots in the transportation logistic industry that makes that required. But, again, I think one of the things is I don't know the nitty gritty and certainly not part of the classified review on DP World, but they will be the third biggest terminal operator in the world. And if we are talking about deploying a global system, you want to be able to work with the operators in that system.

So the challenge here is obviously legitimate concerns about what this means for U.S. ports, but in the context that if we are pushing the borders out, we need all the partners we can get. And I think we should leverage this moment to get DP World, along with the other terminal operators, to do more on improving security, instead of throwing them out of the club, essentially being here, and then we have got to work with them in any event.

I am trying to be pretty pragmatic about this, and I know it is not what is driving———

Mr. DEFAZIO. Right. Well, I mean, I guess I question whether the UAE would be the partner I would look for in having a global system of security.

Mr. FLYNN. They will have the system, so, in my view, you don't look at the ownership issue, you say will you put in place this equipment and do you let us access to the data, is it maintained? And when they are not, then there is some leverage that you use there. So you work with the partners you have.

Mr. DEFAZIO. But I am just intrigued by your comments about an honor system, which seems to me—I mean, we are so reliant upon essentially the bills of lading. You know, I mean, I don't know if you are familiar with the crew issue, but it was sort of the———

Mr. FLYNN. It is an honor system there as well.

Mr. DEFAZIO. Right.

Mr. FLYNN. I mean, 96 hours you list the crew. We hope they put them all in and they spell them right; and these are complicated names, often, to spell. And, again, there is no underlying intelligence that supports most of that, so it is a problem.

The real issue is not so much that we will have a single incident. The real issue for me is we will have an incident—it is almost inevitable—and our reaction, because these programs aren't as robust as they need to be, will we have these cascading—we will pull up the drawbridge and we will end up causing ourselves much more harm than the terrorist cause themselves.

So we need to keep that duality in mind here. It is both trying to deal with the threat, but also the threat ourselves—the threat of damage that we will do to ourselves by not having adequate systems in place that will pass the smile test for the American public post the event.

Mr. DEFAZIO. Thank you.

Thank you, Mr. Chairman.

Mr. FLYNN. Thank you.

Mr. LOBIONDO. OK, thank you, Dr. Flynn, very much. We appreciate it. Thank you for continuing to be such a strong advocate. Please keep shouting.

Mr. FLYNN. My apologies to the rest of the panel for taking your time.

Mr. LOBIONDO. Dr. Carafano.

Mr. CARAFANO. Thank you, Mr. Chairman. I have submitted a statement for the record, and, if I could, I would just like to make five very brief comments. And thank you for trying to accommodate my schedule. I hope to get over to the White House for the signing of the Patriot Act, which I think is something that will make us a lot safer.

I share and I validate the Congress's concerns and frustrations with the manner in which the Administration handled the Dubai World Ports deal and particularly the lack of notification and infrastructure. And I think we all share the good news here, that we have America's attention, and I think simply most Americans don't realize that global maritime system is simply the lifeline of the American economy. I mean, the internet could crash; we could ground all the airplanes tomorrow; and pretty much the U.S. economy would still be there. But if we stop moving goods and services out of this Country by sea, this economy would simply grind to a halt.

And I admire and commend the Chairman and everyone on this Committee for all the work they have done, realizing the number of vulnerabilities that are out there and the spade work that is required to close them and the enormous amount of work that is left to be done.

My approach to maritime security has been the same with my approach to all the aspects of strategy in the long war, and I have always argued there are four components that you have to have in every aspect of your long war strategy, that is: security, promoting economic growth, protecting the civil society and civil liberties, and winning the war of ideas.

And if you have any security solution that doesn't meet all four of those criteria equally well, then you have got a bad answer and you need to go back and start over. And I would hope that the Congress would use this kind of criteria as they look forward to determine what are the next and most important steps to take.

I have three, my top three on the list of what I would do in maritime security. Number one is simply fix the Coast Guard first. The Coast Guard is involved in every aspect of maritime security, and unless they are fully funded and have all the resources they need, everything else really hangs on that skeleton. And I think this is not just about funding Deepwater, which I think if the Administration funds this at anything less than $1.8 billion a year, it is inadequate.

But I think it is time to have the conversation about building the kind of robust, specialized law enforcement capability tracks in the Coast Guard, building specialized special operations capabilities in the Coast Guard that are equivalent of every other service's, building, of course, security professionals, a degree of expansion in the Coast Guard that we simply haven't seen, and actually bringing to fruition some of the concept of maritime domain awareness.

Number two would simply be we need better commercial information into the targeting process before containers are loaded on ships. And I think that commercial information is available. I think it would make high-risk targeting a lot more efficient. And that, I think, would be my second priority.

And my third would be international cooperation. I really think that we lost the bubble and that we are not focusing on the weakest link in the system, which is the shippers and ports in the developing world, which are the entre into the system that I think terrorists are most likely to use.

I think there are legislative—with regard to foreign ownership, I think there are legislative remedies that the Congress could do to give more confidence to the American people that these issues are being addressed, and I would point out two very quickly. One is MTSA and the other is the law that governs the CFIUS process. MTSA was simply not designed to think about the notion of changing of ownership and changing foreign ownership.

And I think we have to ask what appropriate amendments could be made to the law that could strengthen our degree of confidence when maritime infrastructure is transferred between foreign ownership or to foreign ownership. And I think there are some common sense things that we could add to the law.

Number one is a requirement that the security officer of the company be a U.S. citizen and have a suitable background check. And I have listed these in my testimony. I will just summarize some of the ones here. Number two is a mandatory review of the security plan by the Coast Guard on notice of an application.

Also, there would be a mandatory requirement, after the application has been approved, that ownership is taken a mandatory requirement that changes have been made to the plan. Mandatory commitments to assist in law enforcement investigations. And, most important, penalties for non-compliance with these measures.

In regard to CFIUS, I think the problem with CFIUS is that the process is just too informal, and that what it needs is a stronger set of regulatory requirements as to exactly what the CFIUS process is supposed to accomplish. I think there should be mandatory regulatory requirements for agencies to obtain commitments where there is significant national security interest involved.

I think there should be penalties in the law established for non-compliance with those commitments. I think that where there is a significant national security interest identified, I think the CFIUS approval should be based on the joint conclusions of DOJ, Department of Homeland Security, and DOD, not a consensus agreement by the committee as a whole. And I think there should be very firm and clear and specific reporting requirements to Congress.

And I look forward to your questions.

Mr. LOBIONDO. Thank you very much. Do you—I am taking that you do share Dr. Flynn's assessment about doing something on foreign shores before containers are actually loaded?

Mr. CARAFANO. I do, but I really oppose this notion that this is about pushing the border out. I think that is really the wrong impression, because that really doesn't actually get you anything. OK, let us say we have pushed the border out and we are 100 percent

confident between Singapore and the United States that we are good to go.

Well, you know what? Singapore is one of the key hubs of global commerce in the world, and if the terrorists get to Singapore and they do something in Singapore or Hong Kong, that is going to affect all of us almost as badly as if something happened in Los Angeles. So we need to get over this notion that it is about pushing security out. That is exactly the wrong impression. What we need to be talking about is about securing the global commons, securing the domain that we all use, that makes us all healthy and well.

Now, you know, in regards to specific solutions, I have to admit I have a predisposed dislike of security screening as a measure, because what you wind up doing is spending 99 percent of your time and resources on things that are not a problem. I mean, this is the problem we have in the aviation realm. We screen—we spend $6 billion a year—that is the budget of TSA—screening people that get on planes every day that we almost know for a fact are no security risk.

And I much prefer security regimes that put the majority of the security resources against the threat, as opposed to mass screening, which I think is very, very inefficient. I have no problem with the mass screening scenario. The problem I have with a specific technology, if somebody can make a sound business case for these technologies, Steve and I totally agree that there has to be two fundamental requirements if we are going to do this. One is that there has got to be a business case for it and two is it has got to be global so it is a level playing field for everybody.

But in terms of where screening of cargo, mass screening of cargo fits in my list of priorities, I, quite frankly, think it is not high, one, because I think mass screening is inefficient, it has high false positives and false negative rates; it puts a lot of drag on the system and actually doesn't give you a lot of security in the end because in a global supply chain, there are so many intervention points that mass screening secures one intervention point, but you get on either side of that point, you are vulnerable again.

So it is a system that can be relatively easily defeated and I think the scenarios that we use to justify it, which is the nuke in the box, I think is among the most implausible of terrorist scenarios. If a terrorist has a nuclear weapon, then he wants—and this is true of every terrorist attack. Terrorists have limited assets, and they like predictability. They like predictability in knowing what they are going to face and they like predictability in knowing the outcome of their attack. And if you look at every terrorist tactic, it is based on trying to gain that predictability.

Well, what is wrong with a nuke in a box scenario is if I have one nuclear weapon, why would I put it on a cargo container which I had no control over in environmental conditions—and there are—when you have a nuclear weapon, or any kind of bomb, you are concerned about environmental conditions—and send it off out of my control?

If I had a nuclear weapon or a deadly biological weapon or a dirty bomb that I wanted to get into the United States or a U.S. port, I would do it the way smugglers do it: I would take it on a noncommercial vessel, I would land in Mexico and I would drive it

across the border. Or I would take it on a non-commercial vessel and I would land it between a port of entry, which is totally unguarded and I would walk it in. Or if I really wanted to blow up the port itself, I would take it on a non-commercial vessel, I would take it into the port and I would blow up the port.

So this notion that we are going to do 100 percent screening to keep the nuke in a box out of the United States I think is just simply silly. You know, if you have an infinite number of vulnerabilities and you take one away, you have infinite number of vulnerabilities minus one. That doesn't really make you much safer.

Mr. LOBIONDO. Do you share the confidence that Customs and Border Patrol indicated in their process of identifying high-risk and then running it through———

Mr. CARAFANO. No, sir, I don't. I think that—I agree with high-risk analysis and screening of high-risk cargo. I don't think that they have access to the kind of information they need to do to do a quality high-risk assessment. And I think Steve and I agree on this, that you have to have information that goes to the beginning of the supply chain.—and I have listed some of these requirements in my testimony—but you have to know the shipper, the country of origin, who packed it. And that kind of commercial information needs to be part of the risk assessment before the container is loaded on the ship.

Now, the other thing I think is very, very important to realize is will risk assessment give you 100 percent confidence? And the answer is no, of course not. But the other thing people have to realize is you are not depending on the risk assessment as your last line of defense. Risk assessment, in conjunction with robust law enforcement and auditing capabilities, that gives you real security.

You know, it is like we don't ask the police to stop every car they see; we say stop the people that break the law. And I think that is what we want here. What you want is you want a high-risk assessment that is going to give a degree of you some confidence in the system, but you can't trust the system. And I think any part of the system that is based on honor is stupid.

I mean, Reagan had it right when he said trust but verify, which meant don't trust anybody. So you have a system which provides high-risk assessment, which gives you some clues, but that is backed up by robust law enforcement and auditing. That is what gives you the confidence that the system is secure, not the screening process itself.

Mr. LOBIONDO. And that is where the critical nature of funding the Coast Guard comes into play?

Mr. CARAFANO. Absolutely. I mean, this is simply silliness. I mean, quite frankly, I mean, to make an analogy, there is a burglar in the neighborhood. You know, Steve's solution is let us wall up all the houses. If there is a burglar in the neighborhood, let us tell everybody to lock their doors and then let us hire some cops to go out and get the burglar.

That is the right answer. And so I think you are right, if there is an Achilles heel or the emperor has no clothes in this, it is that the one institution which really links all this stuff together and makes the system that we have credible is the Coast Guard, be-

cause they touch every aspect of maritime security, whether it is law enforcement or screening or maritime domain awareness, and they simply do not have the resources to make this system legitimate.

Mr. LOBIONDO. You mentioned the Deepwater program, which is certainly near and dear to me, and the funding of it, which certainly has been inadequate, and each year we seem to fight that battle. You, I think, mentioned anything less than $1.5 billion is really a bad mistake. Was I correct?

Mr. CARAFANO. Yes. And I think that is a very modest number.

Mr. LOBIONDO. Have you had an opportunity, up to this point, to review and study how they are spending the money? In other words, with all the challenges of replacing the assets, some of how they are choosing to replace these assets, have you looked at that?

Mr. CARAFANO. Quite frankly—and I think this is actually true for all the services. In many sense they are making poor choices. What they are doing is they are making choices—they are making the choices they can make as opposed to the choices that over the long term would be the most cost-efficient.

You know, for example, if this was a private sector firm, they would say, you know, spending a $5 billion over three years buys you a heck of a lot more than spending $10 billion over 10 years, because, you know, replacing older equipment more quickly, in the long term, just saves you a lot of money. So I think what they are doing is because we haven't accelerated the acquisition of the program, what they are doing is they are not making the cost-effective choices, they are making the most operationally-effective choices.

In other words, they are trying to keep the car from falling apart. You really ought to buy a new car, so instead what they are doing is they are doing things like, well, they are fixing the brakes, you know, just to keep things running. But in the long run that just costs you more money.

So I think that many of the choices that they are doing are grossly sub-optimal because they are dealing with the fiscal realities of having to go out and do their job every day, and they can't buy the stuff they would want to because the stuff they have got has got to work tomorrow.

Mr. LOBIONDO. I understand that. What I am actually trying to get at is I think some of their decisions to spend money on the biggest ticketed items in the range of what they have to do is what I question when they are spending all this money on a couple of huge ships, and they could, you know, be spreading it out and getting a whole lot more bang for the buck.

Mr. CARAFANO. But I think that is part of the—I agree with you, and it is part of the same problem, is they are forcing and making these sub-optimal choices. You know, as we know, the big ticket items get people's attention, and the big ticket items are easy to get funded, and the little—if you have 15 little things, you are much likely to get whittled to death than if you have one big thing.

So I think that we have just given them an impossible job, we have told them to figure out how to do all this, and then we haven't—and then we have kept the checkbook in the drawer and kept them on an allowance. I just can't—it is just unfair to ask

these guys to make smart decisions on the amount of money we are giving them.

Mr. LOBIONDO. The last question, I think, how do we improve the quality and quantity of information that comes into the Customs and Border Patrol through the advance submission?

Mr. CARAFANO. I think that—I mean, that simply has to be done through the international agreement, and I just don't think that we have been aggressive enough in terms of pushing the envelope on this, and I think that Steve is right, the United States has an enormous stick because we are one of the world's largest global traders, and I just think we should be much more aggressive.

Mr. LOBIONDO. OK, Dr. Carafano, thank you very much.

We are now going to move to Mr. Nagle. Thank you for joining us.

Mr. NAGLE. Thank you, Mr. Chairman. Good afternoon. Thank you for inviting us to testify before your Committee on areas where additional efforts are needed to meet the objectives of MTSA. I ask that my full written testimony be placed in the record.

Enhancing maritime security and protecting America's seaports from acts of terrorism and other Federal crimes is a top priority for AAPA and our member U.S. port authorities. Ports handle 99 percent of our overseas cargo by volume, enable the deployment of our military, and serve as departure points for millions of cruise passengers each year.

Let me begin by some comments on the proposed DP World acquisition of P&O ports.

In reviewing a transaction of this type, it is the appropriate role of the Federal Government to determine if there are national security concerns with any proposed business arrangement involving non-U.S. interests, whether that involves port operations or any other business. There should be a rigorous process to appropriately consider and resolve those questions.

AAPA believes that the current 45-day process underway regarding the Dubai Port World's acquisition of P&O ports should be allowed to run its course prior to Congress taking any action either on this proposed arrangement or on any blanket prohibition against a foreign government-affiliated company from providing terminal operating services at U.S. ports.

With regard to individual business arrangements, public port authorities often have leases with terminal operating companies to operate port-owned facilities. These leases typically provide that any assignment of a lease to a successor company in the event of a merger or acquisition must be approved by the port authority. Leases generally cannot be transferred or assigned without permission.

The recent focus on port security has made many question what else this Country needs to do to secure our ports. My testimony today will focus on three areas: one, the Port Security Grant Program; two, the Transportation Worker Identification Credential, TWIC, that has been mentioned this morning; and, three, adequate resources for the Federal agencies primarily responsible for port and maritime security.

Soon after September 11th, Congress established the Port Security Grant Program to provide much needed help to port facilities

to harden security to protect these vital ports of entry from acts of terrorism. While the program has provided much needed funding, it still has several problems. Let me begin with the funding level.

From its inception, the Port Security Grant Program has been dramatically underfunded. DHS has been able to fund only about 20 percent of the identified needs through the applications. AAPA recommends an annual funding level of $400 million for this program. Limited funds have placed huge burdens on port authorities as security projects compete with funds required for maintenance of facilities, channel dredging, and other port expansion projects to meet growing international trade. The biggest impact of funding limitations, however, is a delay in making security enhancements. Limited funds means slower progress.

This low level of annual funding has resulted in DHS limiting the eligibility of the program. Last year, DHS decided to limit eligibility, leaving nearly half of our member ports ineligible to even apply. We support a risk-based system; however, we believe that each port facility that must meet the requirements of MTSA should be able to apply. We are also concerned that limits on eligibility might leave a class of perceived underprotected ports.

The Administration, also as has been mentioned this morning, has sought to eliminate the Port Security Grant Program during the last two years by lumping port security into a broader targeted infrastructure protection program. This is not the time to dilute the focus on port security; it should remain as a separate dedicated program. AAPA is also concerned by the slow pace in making the funds available. For fiscal year 2006, we are still waiting for the application process to open for the port security grants, nearly six months after the appropriation bill became law.

A second priority for AAPA related to port security is quicker implementation of the TWIC. Four years after this requirement was enacted in MTSA, we are still far from implementing a TWIC system nationwide.

The third area AAPA believes should be a priority for port security is ensuring that adequate resources are available for the Federal agencies with primary responsibility for port and maritime security. Again, there has been a significant discussion of this both this morning and in this panel.

The U.S. Coast Guard and Customs and Border Protection are the two key agencies that need adequate resources to address port security. Both have done a great job to address these new challenges post–9/11. Projections on container and passenger volumes, however, show a huge increase at seaports in the coming years. Congress needs to take a careful look at whether these agencies will have the manpower and resources to handle this growth in their security responsibilities.

In conclusion, our Nation and its public ports have made great progress in enhancing port security since September 11th, in large measure due to the actions of this Committee and your leadership in moving forward MTSA legislation. However, we continue to need to make progress in this area. On behalf of the American Association of Port Authorities and our member ports, thank you for the opportunity to be here this afternoon, and I am willing to answer any questions at your time, Mr. Chairman. Thank you.

Mr. LOBIONDO. Well, thank you very much. There are so many different areas to talk about. The port security grant issue is one that has disturbed us a great deal. Depending on what numbers we use, the current requested level of funding from DHS I think last week looked like it would take some 60 years before we come to even the bottom line of what was required.

In the meantime, you are expected to continue to do more, you are just given more and more mandates. And we are hoping that we can get someone's attention or the secretary and Mr. Baker carries back this message. He heard some pretty strong messages last week in Armed Services, and I think he did hear again today.

But I would like to ask you some specific questions about how do you interact with the Coast Guard and other DHS agencies to carry out the common mission of the port security?

Mr. NAGLE. I think as was relayed this morning, certainly with Representative Coble's discussion as far as the four-legged stool, it definitely is a partnership effort between the Federal agencies. Again, certainly Customs on the cargo security side and Coast Guard on the vessel and facility security side have primary responsibility. However, the public port authorities have a role in that, the terminal operators have a role in that, as well as the private sector that are involved.

As indicated, all of the facility operators, whether they are public agencies or private, do need to prepare and provide a facility security plan that is reviewed and approved by the Coast Guard. And then—so you have a facility security plan process that is approved and in place and ongoing. You then also have essentially a local port area maritime security program that is chaired by the Coast Guard captain of the port, and the local port authorities are part of that local security committee that looks at the broader, beyond the individual facilities, to generally the port area. And there are—also as part of that there are studies, analysis, et cetera, to determine and make recommendations as far as what security or enhancements are required to address security in the broader port area.

Mr. LOBIONDO. Do you receive sensitive or classified information from the Coast Guard or any other Federal agency regarding potential threats to homeland security at our ports?

Mr. NAGLE. We, as AAPA, do not receive sensitive security material. If there are—and in many cases at the local port authority the facility security officers or others that may well have security clearances would be able to receive that information, but as a general course of matter, and certainly through the Association, no. We are on certainly the correspondence with Department of Homeland Security regarding security sensitive information that they are able to provide that we can provide through the Association to our local individual members, but not secure information.

Mr. LOBIONDO. I take it from your testimony that the top two items that you would suggest the Federal Government needs to get on quickly would be additional port security grants and then the TWIC card?

Mr. NAGLE. I would say from the port authority's perspective, I think all three of the areas are—I would certainly indicate as equal, the two you mentioned as well as the additional resources

for Coast Guard and Customs. Again, the first two are principally looking at the security of the port facilities and making sure that the people that are on that facility are who they say they are and have authorization to be on that facility and to take cargo either onto or off of that facility as appropriate.

The third area as far as the Coast Guard and Customs is in the essentially outside of the terminal gates responsibility regarding cargo and vessels that are entering the U.S. And as has been mentioned, whether you defining it as pushing the borders out or however you define that process, certainly there is significant value and interest in moving the determination of any either vessels or cargo at risk before it reaches the U.S. port. As Mr. Oberstar mentioned earlier, certainly, while it is the last layer of defense, doing something, radiation portals at the U.S. port in many instances that could potentially be too late.

Mr. LOBIONDO. Could you say what is the biggest risk, exposure, threat because of lack of port security grants? What gaping hole is that leaving that the private side is not able to pick up? We know there is an enormous number of dollars that are necessary to even come up close. How would you rank what are the areas that are most at risk because of lack of port security clearance?

Mr. NAGLE. The areas that our members tell us are the areas that they have identified as still requiring significant enhancements at the funding because of lack of funding is being at least delayed, if not being able to be done, period, are in the areas of access control—again, whether that is physical access controls or credentialing systems, et cetera, that, again, are in many having to wait to be implemented because of the TWIC, not knowing what their requirements are going to be from the Federal TWIC to make sure that they are compatible with what a local port authority would do in terms of credentialing, et cetera.

But access controls. Perimeter security, whether, again, that is the physical perimeter security by personnel or by fencing, lighting, video surveillance, certainly utilizing technology to better being able to provide surveillance of the facility. Communication systems, being able to communicate amongst the various—whether it is the port authority security personnel, local law enforcement. In general, those would be the first responders in any incident related to a port or maritime environment. Communications command and control systems are certainly recognized as very important.

And probably the final area that again is still a subject of particular interest is water-side security. Again, the Coast Guard has primary responsibility for that, but with their limited resources, they are obviously not able to be at every single facility at all times. So looking at the opportunity of either patrol boats and either radar or sonar detection devices that help provide a level of security regarding any intrusion from the water side. Those are, I would say, the four areas that our members have identified as most in need of additional funding.

Mr. LOBIONDO. So are you saying that if we had an incident with one of your members at one of the ports, that there would be an inability for the different entities involved to communicate directly?

Mr. NAGLE. I would say that there are still cases that you are still looking at the compatibility—I think that was certainly given

the experience in September 11th, the inability of the various responders to be able to communicate———

Mr. LOBIONDO. What I am getting at.

Mr. NAGLE. Yes. Certainly there has been progress made in that, but I would not say that there has been certainly conclusive determination of what that interoperability between systems is between all those local responders. In many cases they are outside the control, obviously, of either the port authority or the Federal, say, Customs, Coast Guard, et cetera, because you are coordinating with the local and State agencies that would have their own communications systems. So it is a matter of trying to coordinate all of those various potential first-responders and be able to communicate amongst themselves. That is still an issue.

Mr. LOBIONDO. I have a hunch you are being pretty kind in your description of how that has come together and where we are with all that. Last question I have, do you have any estimate of what your members have spent, either on their own initiative or mandated, in port security that has been non-governmental help?

Mr. NAGLE. I can't give you an actual figure, but essentially we have been able to determine—I would say it is beyond what is provided in the Port Security Grant funding, which has been, to date, actual, $707 million, and then with the additional $175 million that will be coming out in this upcoming round, so roughly a little over $880 million. In general, it looks like there has been, I would say, hundreds of millions of dollars spent by the port authorities in addition to that figure.

I think the numbers that were referenced this morning, the $5.4 billion estimate was only for facility security. There was some intimation that that was for a broader level of security beyond facilities. The estimate, when Coast Guard looked at the costs of implementing MTSA on facility security was $5.4 billion over 10 years. The first five rounds of grants, there has been a total identified needs applied for of $3.8 billion, and only $700 million has been applied. That is the 20 percent that I was referencing in the reference that you made as far as how little has been provided to public ports.

So I think there has been some level of correspondence between the level of identified needs that have been applied for and that Coast Guard estimate that gives us the general feeling that that total figure of $5.4 billion seems to be certainly within the ballpark.

Mr. LOBIONDO. I thank you very much. We apologize and we thank you for adjusting your travel schedule. We understand that you have missed your original flight and had to reschedule, and we very much appreciate that. And if in fact you need to go, please feel free.

Mr. NAGLE. At this point, because of the switch, I am fine, and if you would prefer for me to stay for the panel, I would be happy to do that.

Mr. LOBIONDO. Might be an additional question.

Mr. NAGLE. OK, sure.

Mr. LOBIONDO. OK.

Mr. Scavone, please.

Mr. SCAVONE. Thank you, Mr. Chairman. I have submitted my comments for the record. I know that you, sir, heard my remarks

at the Armed Services Committee last week. I will mention a few points relative to my comments today and try not to be repetitive.

In addition to being also responsible for security at P&O, I also serve on the Board of the National Association of Waterfront Employers, who did submit comments on port security to the Senate Commerce Committee today, and with your permission, sir, I would like to send those into this Committee for its record.

Mr. LOBIONDO. Without objection.

Mr. SCAVONE. I would like to offer first a few comments on the security of the global supply chain.

Of late, we have become accustomed to hearing that our ports in the U.S. are the most vulnerable points of entry. This tends to lead to the conclusion that the ports themselves are the location where security needs most to be enhanced.

That is not a correct conclusion. Our ports in the U.S. are already the one point in the supply chain over which we have the most control. It would be more accurate to say that if the security of the supply chain in a foreign location should fail, the place where we in the U.S. will be first exposed to that failure would be in the U.S. port. However, no amount of security on the part of the terminal operator in that U.S. facility will change that fact.

Therefore, the enhancement of the security of our U.S. ports and, by extension, our homeland, is best accomplished by improving the security at the point of origin. We have heard today about programs like the 24-hour rule, C-TPAT, the CSI program, which have all contributed to that goal. If efforts will be made to continually improve our security, this is where the focus must remain, to include such matters as the integrity of container seals, the improved capability to conduct non-intrusive inspections at port of loading, ideally at the direction of U.S. Customs, and the upgrading of Customs' Automated Targeting System.

Some of these objectives will experience substantial progress via the simple decision to devote more resource to them, which has been discussed already today. Others would require a global program joining the governments of virtually every trading company with carriers, terminal operators, technology vendors, and international standards bodies such as the International Standards Organization, or ISO, which leads me to a few points about foreign ownership.

The fact that foreign interests own many of the companies that manage our terminals in the U.S. has recently, as we know, become a major point of discussion. The focus has been on the extent to which such ownership may impact the security inside our terminals. The answer is it does not impact the security function at all. We have already heard that the Coast Guard, Customs, and the port itself continue to be responsible for that security. We, as terminal operators, do have responsibility to have access controls to our facilities, but that function is approved, monitored, audited, and enforced by the Coast Guard.

The terminal operator has no role in verifying or inspecting the declared contents of any container entering the United States. A terminal operator does not open a container to verify its contents. Inspection is performed exclusively by U.S. Customs under its own

supervision. And no container leaves a U.S. facility until U.S. Customs indicates that it is free to go.

In every case of which I am aware, foreign ownership of terminal operating businesses in the U.S. is conducted by U.S. subsidiaries employing predominantly U.S. citizens and U.S. labor. However, under no circumstances does this permit the foreign shareholder to control any port or terminal in the U.S. Obviously, the shareholder will control indirectly the overall business strategy of the company, but like any business, it will be subject to the laws of the countries in which it operates, and it may only exercise its influence within those limits.

If you accept that the security at the originating end of the supply chain is the area most requiring attention, you will then recognize that the participation inside the U.S. of the major global terminal operating companies of the world, alongside our U.S. terminal operating companies, permits us to have a much broader global cooperative effort to address the ways and means to enhance the security of that supply chain.

For example, the global operators who also have a U.S. presence represent possibly the single greatest resource in the effort to deploy scanners in foreign countries and to supply to U.S. Customs the scans of every container they move onto a vessel bound for the U.S., which in turn addresses the question of intervention that Dr. Carafano raised, where you could potentially intervene at any point along the way. But if you check the box before it is actually loaded onto the vessel heading for the U.S., there is no additional intervention after that.

A question was raised about the impact of DP World deal on the security of the New York cruise terminal. By agreement with the Coast Guard at the New York cruise terminal, the role of the facility security officer is actually filled by Michael Stapleton Associates, a private security firm composed of ex-NYPD detectives and officers. That firm, in cooperation with the Coast Guard, prepared our facility security plan and they operate it.

The Coast Guard has been highly complimentary of our security measures there, which include measures beyond those required by the regulations, such as canine patrols, and nothing about that is going to change. Further, we do not have access to passenger lists or crew lists; those are kept by the cruise lines and CBP. The sailing schedules are on the cruise line Web sites; thus, the sale of the P&O parent company in London would have no impact on the security at this terminal.

In Beaumont, Texas we load military vehicles on vessels chartered by the military. We use longshoremen to do it. Numerous military personnel are always present to supervise that operation. The only information we receive about the cargo is a written list of equipment to be loaded. If anyone wanted access to this information, they would only have to stand outside the terminal fence and count what goes in and out, the point being the information we have is not confidential to begin with.

In conclusion, Mr. Chairman, when we discuss risk in the supply chain, I believe it is important to distinguish between risks that exist today and risks that might somehow be created if P&O is sold. I believe we have seen that those who know how security real-

ly works are virtually unanimous that this sale is not an issue from a security standpoint.

Thank you, Mr. Chairman, for the opportunity to submit these comments today.

Mr. LOBIONDO. Thank you.

Mr. Brown, thank you for your patience. Thanks for making a very long trip, and I am waiting for your remarks.

Mr. BROWN. Thank you, Chairman LoBiondo. And thank you, Member Filner and the rest of the members of the Committee. I want to thank you for having the opportunity to come and speak here and for the invitation.

My name is Gary Brown. I am a third generation longshoreman in the Port of Tacoma, Washington; roughly 37 years down there. I am also privileged to serve as the security liaison officer for the International Longshore and Warehouse Union. And in this capacity I have received numerous security certificates and certifications from the Coast Guard. I have taken my class with FEMA and I was very fortunate to have taken a class that was sponsored by the U.S. Attorney's Office for anti-terrorists. So that is a little bit of my background.

Also, on February 14th and 16th of this year, I organized a port security training session for the ILWU and its members in conjunction with the Pacific Maritime Institute, which is one of the few government recognized and organizations institutes. I had longshore workers from every local up and down our coast, the whole International, including two members from Hawaii, and they were trained on a facility, company and vessel security regulations required by the Coast Guard.

I had the distinct pleasure of having retired Captain Danny Ellis, Coast Guard, and Assistant Chief AD Vickery, Seattle Fire Department, who has been involved in several—I guess he is the grandfather, as they say, or the founding father for the Marine Terrorist Response Program in Puget Sound, and which is going to be nationwide. They have helped me with my program and were nice enough to have the Coast Guard send two people to speak at the class, Customs sent two people, and along with, like I said, the Fire Department, first responders, and a gentleman that was retired from the Treasury Department to speak on some anti-terrorist things for us to be watching out for.

So it was a very good class. All the members were certified and this was totally funded by and paid for by the ILWU. We paid and initiated for this because our employer had failed to conduct a proper training course which is required by the Coast Guard. And on that note there, that is where we are at with our training, and if we could get any help with any funding, we would appreciate it.

Just to touch on the Dubai Ports deal as far as the International Longshore and Warehouse, where we stand is that we fully support the bipartisan calls in Congress for the Bush Administration to direct a committee on the foreign investment to conduct a full 45-day investigation, because our seaports are part of our global economy.

The ILWU believes that we should not rush to open the doors for such assets to companies owned or operated by foreign countries where there were serious concerns with existing terrorist activities and funding. Therefore, we are urging that the decision for the ap-

proval be based on national security interests of the United States, and not on commercial interests of any one company or one country.

We also urge the Federal Government, including Congress, to focus its attention beyond the controversy over the one future commercial contract and to recognize and correct immediate major deficiencies of the security that exists today in American ports. It is the current lack of effective port security since the terrorist attacks of 9/11 that is the real concern of all the dockworkers and millions of Americans who live within close proximity of our Nation's ports.

To touch on that, you have heard several discussions from everybody today on panel one and the gentleman here was on seals. Seals was something that we as longshoremen used to conduct, physically check the seals, and now they are done via the cameras, and the cameras, you can't see the number and you can't tell if it is secured. It is a severe problem.

Another problem is empties. This is something that was brought up and a lot of people wonder why empties are such a problem. Empties are a perfect example of an access for somebody to use to put something in to transport something in, because they are not examined. We used to examine them for several reasons: number one, to make sure they were empty; number two, to make sure they were clean, because a lot of the customers require a certain type of container; and we also checked for structural damage, which is a safety factor.

And not only that, but we have found—I personally found 25 Chinese in a container one night that was an empty, and, fortunately, the only reason we found it was because we were getting ready to stack it in the storage area, which is where it would have probably stayed for about four or five days. And for some reason it was close to lunch time, so I told my driver just leave it on the ground, and within five minutes I got calls on the radio that there were people running all over the terminal down there, so I caught one of them and that is what I found out, that they had been in that container, it was an empty.

And another problem we have is we don't have, like on our shipping list. They talked about—the gentleman earlier talked about the honor system, and we work with several of those companies that are on this honor system, but these same companies we have containers, if we get a discharge list of approximately 450 containers, we have 462 come off. That is 12 extra. And they are not on the list.

Well, according to regulations, and if everybody was to follow the rules, you call Customs, because now you have got a break in security; you have got 12 extra containers. Unfortunately, the companies' response is just write those numbers in and worry about it later on. And this is something that we deal with every day, and this is not acceptable.

We talk about rules and regulations, and they are not being followed. And like I said, with the seals, with the loads, with the empties, we have loads coming off ships now and it is such a fast paced business that we are getting—if you happen to look at some of these manifests on there, they are listed as dummy, D-U-M-M-

Y, because they don't want to take the time to stop and verify that container, so they come through as dummies.

And I have had several meetings with the companies and I said, you know, what is the process with that, because you have these dummy containers? Well, what they will do is they will run it through and the computer will pick it up, where, in the old days, I had—I am a marine clerk, and I had the manifests, I would verify these things; I would verify the seal, I would verify the container, and at one time we knew what the contents were. And we don't have access to any of that anymore, and this is all done through the computer process, and this is what our concerns are at, because we don't have access to that anymore.

And we have had several where there was an incident in Long Beach where the container blew up. Had we had access like the old days, what we are supposed to do is check that container, we would have found out that it had propane in it. But on this list that was set out, it was FAK, freights of all kinds/dummy. And luckily nobody was killed, but it blew the container doors off and, my understanding, it blew things about 40 feet behind it. And these are our concerns, you know, the empties, loads, and, of course, now we have at our gates now we have—to give you a quick incident, if I could.

We used to be down in the lanes. When a driver would pull in, he would give us his manifest, we would double check to make sure the container was right, the seal number was right, plus it was locked; you would physically grab it and pull it. And if it was placarded with "Hazardous," you would walk around and make sure it has all the placards on it because of Coast Guard regulations.

Well, now a driver pulls up and he gives you the seal number over the phone. And, of course, your camera on it shows—you look in your camera and the density and stuff, it just shows a glob. There is no way you can verify the number; there is no way you can verify if that seal is actually secure.

And in this one incident, the gentleman came out of Canada and it was hazardous, and he pulled up to the lane down there and I asked him the seal number, and he gave me a seal number. Well, he had had placards on it, so I had to go down and walk around it.

Well, when I got to the rear of the container, there was no seal. And I walked up to the driver and I said, you gave me a seal number over the radio; there is no seal on the door. And he just shook his shoulders. And I said, did you check the container before it left the dock in Canada, and he goes no. And, of course, he didn't stop because he used a NAFTA lane coming across the border, where he doesn't have to stop.

And I said, did you stop anywhere along the way? And he goes no. And I said where is the seal? There is no seal on this. He says, I don't know. So at this point I had just finished one of my classes, and, of course, that was a red flag, foreign container, hazardous, no seal, breach of security. And so the response was the protocol is to call Customs.

Well, unfortunately, when I called the terminal operator and explained to them—that is their job to call Customs—their response was throw another seal on it, it is going to miss the ship. And I

said, no, we have got a severe breach here, we have to call Customs. So I was chastised for that, but I called Customs and that container was taken aside. So I don't know what happened at the end of that, but this is just things we go through daily down there as far as security. And it is of great concern because, like with the empties, I like to touch back on that.

It is also the empties coming in from inside, not just the ones coming off the ship, because we have found tons of things in there, and the gentleman eluded earlier about the empty containers and the drivers. Drivers come in and a lot of these companies the terminal operators, a couple of them own their own trucking companies now, so they actually have a little kind of a card they put on their dashboard, and they are just in and out of the terminals.

And there is no way you can monitor these guys. I have seen drivers come in with giant sleepers, and just out of the corner of my eye I catch them where they are parking in the terminal, and I see two or three guys pile out of this sleeper. You know, they are helping them with the container or they are lose on it. Those aren't being inspected and the drivers aren't being I.D.'d, you know. That is another concern of ours. And since we aren't checking empties any more, you know, the people ask me, they say why would you check an empty? Because I told them I found people in there, I found cargo in there.

And, you know, the stuff that—we are looking at loads and we are looking at seals, you know, this is where we are concentrating, but we have also got to concentrate on those empties because as we know, you know, the people that want to do us harm are very methodical, and they are very inventive, and if they can see we are paying attention to loads and seals and all this stuff, but not on empties, because these empties are loaded on the ship next to the loads and the empties are loaded on and off trucks just as they do as the loads, and if we are not paying attention to those empties, it is a golden opportunity for these people.

And I say from the enemy within, because, as we all know, unfortunately, the terrorists that attacked us on 9/11, that attack occurred within the United States, within our States, and I believe after some of the classes I have been and listened to some of the people, that there are people in this Country that have pretty much established themselves, and for them to put—if their goal is to destroy or disrupt our docks, you know, they could very easily build a bomb or whatever they want in Scottsdale, Arizona and ship it, and once it is on the terminal ignite it. So the concern from inside as well as outside is very sincere.

And like I said, you have my statement, and I thank you for the time, if you have any questions.

Mr. LOBIONDO. Thank you. What would be in your order of priority? You mentioned a lot of things, but the top three things that we need to do from your perspective to better secure the ports?

Mr. BROWN. Well, like I said, Mr. Chairman, the sad part is that we used to do the job of, like I say, checking the seals and checking empties. That is something we don't do any more. We actually had letters from terminal operators that don't want it done any more. I have been to several meetings on committees and stuff where people have asked me, you know, why did you guys quit doing that,

and I said, well, it wasn't us. And they thought it was pretty silly. And in this day and age, after what we have had happen, we should be a little bit more vigilant and a little bit more checking this stuff, and it has just gone backwards.

So actually the checking of the seals, the documentation, and—because, like right now, you cannot—if a container pulls up to the terminal, we are looking at the seal now with a camera, and you can't tell the number; you have to take the driver's word for it. And, unfortunately, you can't go find out if that thing is—I did a test with a news reporter up in our area about a year ago, and I told them, and they said, well, what is the big hoopla about seals, once they are sealed?

Well, there was a broken seal that had already been cut, and I went over and put it on a container, used my chewing gum, put the tip back on it and stood back and said, now look through your camera. Does it look like it is sealed? He said yes. So I went over and popped it off. And when we were doing it, you know, you give it a good yank and make sure and make sure the number matched, all that stuff, and we would look for any abnormalities on that stuff.

And we are just not doing that anymore, and that is the big concern, because, you know, people—like I said, people in there, if they wanted to store something in there—but the seals and the empties and probably the drivers that come, the truck drivers. A lot of these guys are around the terminal, they are not—you know, they are not monitored. And you get on a busy terminal down there and you have got a couple thousand people rolling around there, it is impossible, absolutely impossible to catch.

And the only time we come across, like I mentioned earlier with the empties coming off the container ship, that is when I call or have my members call Customs or Coast Guard, and they will respond. But we have to catch them. And on a busy day, you know, like I mentioned before, the Coast Guard and Customs, those people are very thin; they can't be at every port, they can't be at every ship.

And this is kind of like when—that is what we are down there for. And with this training and stuff, you know, we figure, you know, we are down there daily, we know who belongs or who doesn't, you know, and we are a valuable resource working with the first responders.

To give you a quick instance of why we want to enhance our training and be there to help is they had a ship fire up in Seattle, and the Fire Department—I mean, it was an intense fire, and they stood on the dock and they weren't going to go aboard because there was a container right on the middle of the deck and it had placards on it. And they were waiting for that. They didn't want to get on board and have that thing blow up and then kill a whole bunch of people.

And nobody knew what to do, but the longshore, one of our members had gone back up in the crane and hoisted that container out of the fire, got it off the ship they were in. So this kind of brought on our program, because I had worked with a lot of first responders and like the fire chief says, he says, I don't know how to drive a crane and you don't know how to drive a fire truck, but together,

if there is an incident, an event, you know, we will make a hell of a partnership. And that is kind of where our program has gone.

Mr. LOBIONDO. Thank you.

Mr. Scavone, if the acquisition of P&O ports by Dubai Port World is approved, would Dubai Port World also have direct control over stevedoring operations in these 16 additional ports?

Mr. SCAVONE. Yes. Well, P&O Ports, which would remain a place as a U.S. company with U.S. employees operating in the U.S., yes. They would be the ultimate owner of that company, about five or six corporations up the chain.

Mr. LOBIONDO. And how does P&O Ports' involvement at U.S. ports where it operate terminals differ from its operation as a stevedore in the 22 U.S. ports?

Mr. SCAVONE. The 22 locations I think you are referring to, Mr. Chairman, include the 6 where we actually manage terminal facilities. All this information is on our Web site and has been for a long time. In most ports we serve purely as a stevedore, simply to remove the cargo from a vessel and put it down in the terminal.

But in those cases the terminal itself is operated by, for instance, a port authority that is an operating port authority like Houston or Norfolk, and that entity would be the one responsible for the security of the terminal facility and for the preparation of the facility security plan with the Coast Guard; whereas, in places like Port Newark, we also operate the terminal itself.

So in addition to stevedoring the vessel, we manage the terminal facility and then it becomes our responsibility to agree with the Coast Guard a facility security plan, which is primarily the access controls to that facility for people and vehicles under the supervision and direction and enforcement of the Coast Guard.

Mr. LOBIONDO. OK, gentlemen, I thank you very much. It has been very helpful and informative. We appreciate your patience.

And the Committee stands adjourned.

[Whereupon, at 1:37 p.m., the subcommittee was adjourned.]

TESTIMONY OF ASSISTANT SECRETARY STEWART BAKER
BEFORE THE HOUSE TRANSPORTATION AND INFRASTRUCTURE
COAST GUARD & MARITIME TRANSPORTATION SUBCOMMITTEE
U.S. HOUSE OF REPRESENTATIVES
MARCH 9, 2006

Mr. Chairman, Ranking Member Filner, and Members of the Committee: I am pleased to be here today to help discuss the critically important issue of port security.

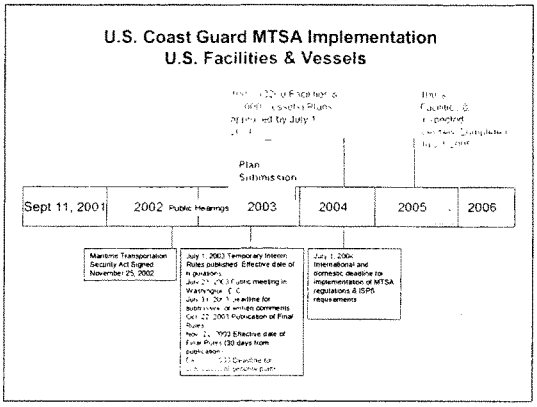
I am also available to help clarify any questions you have about DHS's role in the Committee on Foreign Investment in the United States (CFIUS) and DHS's consideration of the Dubai Ports World (DP World) acquisition of the British-owned Peninsula and Oriental Steam Navigation Company (P&O) and P&O's wholly owned U.S. subsidiary, P.O. Ports North America, Inc.

As DHS's Assistant Secretary for Policy, Planning, and International Affairs, I play a key role in both DHS's ongoing efforts to continue to strengthen port security and DHS's participation in the CFIUS process.

DHS's Role in Ensuring Strong Port and Maritime Security

DHS continues to implement a multi-layered strategy to keep our ports safe and secure. Utilizing the expertise of our bureaus – particularly the United States Coast Guard and U.S. Customs and Border Protection – the private sector, and state and local authorities, we have made great strides since 9/11 to ensure that there are protective measures in place from one end of a sea-based journey to the other. With the President's FY 2007 Budget request, total DHS funding for port security activities since FY 2004 totals nearly $10 billion.

As the lead federal agency for maritime security, the Coast Guard routinely inspects and assesses the security of 3,200 regulated facilities in more than 360 U.S. ports at least annually in accordance with the Maritime Transportation and Security Act (MTSA) and the Ports and Waterways Safety Act (PWSA). Every MTSA-regulated U.S. port facility, regardless of the owner or operator, is required to establish and implement a comprehensive Facility Security Plan (FSP) that specifically addresses the vulnerabilities identified in the facility security assessment and details measures and procedures for controlling access to the facility, including screening, designating employees with key security responsibilities, verifying credentials of port workers,



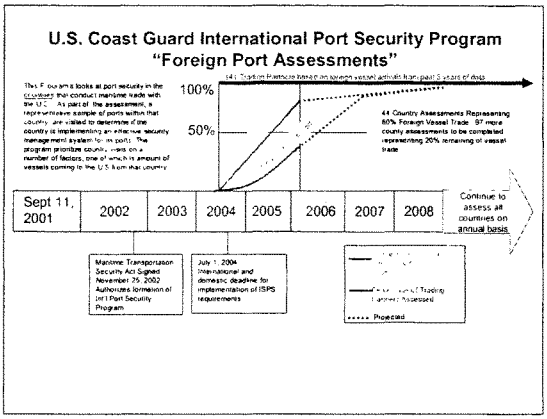
inspecting cargo for tampering, designating security responsibilities, quarterly training, drills and annual exercises, and reporting of all breaches of security or suspicious activity, among other security measures.

Working closely with local port authorities and law enforcement agencies, the Coast Guard regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance.

In accordance with MTSA, the Coast Guard has completed verification of security plans for U.S. ports and port facilities and vessels operating in U.S. waters. Specifically:

- Port Threat Assessments for all 55 militarily or economically critical ports have been completed. The Coast Guard has developed 44 Area Maritime Security Plans covering 361 ports, the Great Lakes, the Inland and Western Rivers and the Outer Continental Shelf region.
- The Coast Guard completed initial security plan verification exams on all 6,200 U.S. flag inspected vessels on July 1, 2005.
- The Coast Guard has completed 2,400 verification examinations on uninspected vessels regulated under the MTSA, and is on track to complete all 4,800 by December 31, 2006.
- The Coast Guard has reviewed and approved 3,200 facility security plans.
- The Coast Guard has approved 60 offshore facility security plans.

In addition to the Coast Guard's broad authorities for ensuring the security of U.S. port facilities and operations, the Coast Guard worked through the International Maritime Organization to develop the International Ship and Port Facility Security (ISPS) Code. Through the International Port Security Program, the Coast Guard has partnered with other nations worldwide to ensure compliance with the ISPS Code. The Coast Guard has assessed 44 countries, which are responsible for 80% of the maritime trade to the United States. Of those 44 countries, 37 have been found to be in substantial compliance with the ISPS Code. The seven countries that are not in substantial compliance have been or will soon be notified to take corrective actions or risk being placed on a Port Security Advisory and have Conditions of Entry imposed on vessels arriving from their ports. The Coast Guard is on track to assess approximately 36 countries per year.



The Coast Guard has also taken multiple steps to enhance our awareness in the maritime domain. The 96-hour Notice of Arrival regulation allows sufficient time to vet the crew, passengers, cargo and vessel information of all vessels prior to their entering the US from foreign ports. The Coast Guard also has expansive authority to exercise positive control over a vessel intending to enter a port or place subject to the jurisdiction of the United States. Since July 2004, the Coast Guard has boarded 16,000 foreign flag vessels for security compliance with the ISPS Code and the MTSA. Out of those 16,000 boardings, the Coast Guard imposed 143 detentions, expulsions or denials of entry. In addition, the Automatic Identification System (AIS) has been fielded at 9 ports with Vessel Traffic Service systems and allows the Coast Guard to identify and track vessels in the coastal environment. Long range tracking, currently in development, will enable the Coast Guard to identify and track vessels thousands of miles at sea, well before they reach our coastal zones. Likewise, the Inland River Vessel Movement Center provides critical information about the movement of hazardous cargoes along our Nation's inland rivers.

The Coast Guard has increased its operational presence through a number of other initiatives. For example, the Coast Guard has established processes to identify, target, and have conducted 3,400 security boardings on High Interest Vessels. These boardings included 1,500 positive control vessel escorts to ensure these vessels cannot be used as weapons of mass destruction. The Coast Guard has also established 12 Maritime Safety and Security Teams and enforced hundreds of fixed and moving security zones to protect Maritime Critical Infrastructure and Key Assets (MCI/KA) and Naval Vessel Protection Zones (NVPZ) to protect U.S. Navy and Maritime Administration vessels. Further, the Coast Guard is developing a Risk-Based Decision Making System, to be implemented this year, which will help prioritize High Capacity Passenger Vessels (HCPV) escorts. Although initially developed for high capacity ferries, its application is being expanded to enhance current security measures for other HCPVs: ferries, cruise ships, and excursion vessels carrying 500 or more passengers.

The Coast Guard is also working closely with various other agencies to implement the National Strategy for Maritime Security, and its eight supporting plans. Together, the plans provide the road map for the integration of national efforts in supporting the four primary pillars of maritime security: Awareness, Prevention, Protection, and Response and Recovery. As DHS's executive agent for implementing and updating plans related to Maritime Domain Awareness (Awareness), Global Maritime Intelligence Integration (Prevention), Maritime Transportation System Security (Protection), and Maritime Operational Threat Response (Response/Recovery), the Coast Guard, in cooperation with other stakeholders, is leading efforts to increase the coordination, effectiveness and efficiency of existing government-wide initiatives.

CBP Efforts Overseas Protect our Domestic Ports

In close coordination with the Coast Guard, the mission of the U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the United States by eliminating potential threats before they arrive at our borders and ports. For example, through a program administered by CBP, the Department has implemented the

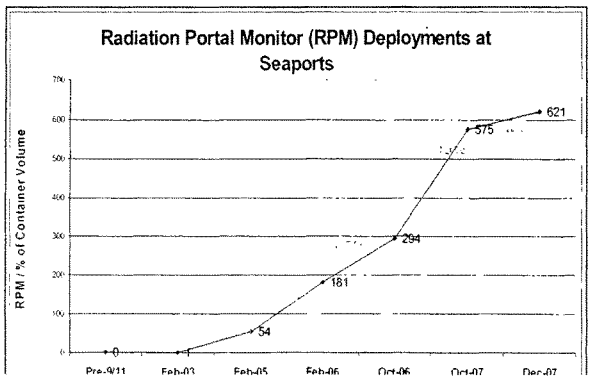
24-Hour Advanced Cargo Rule, requiring all sea carriers, with the exception of bulk carriers and approved break-bulk cargo, to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States. Failure to meet the 24-Hour Advanced Cargo Rule results in a "do not load" message and other penalties. This program gives the Department greater awareness of what is being loaded onto ships bound for the United States and the advance information enables DHS to evaluate the terrorist risk from sea containers.

Similarly, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiatives bolster port security. Through CSI, CBP works with host government Customs Services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. In addition to the current 42 foreign ports participating in CSI, many more ports are in the planning stages. By the end of 2006, we expect that 50 ports, covering 82% of maritime containerized cargo shipped to the U.S., will participate in CSI. The table above shows the Department's substantial progress in expanding the CSI program since September 11, 2001.

Through C-TPAT, CBP has created a public-private and international partnership with nearly 5,800 businesses (over 10,000 have applied), including most of the largest U.S. importers. C-TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security. CBP reviews the security practices of not only the company shipping the goods, but also the companies that provided them with any services.

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

CBP also uses cutting-edge technology, including large-scale X-ray and gamma ray machines and radiation detection devices to screen cargo. Presently, CBP operates over 680 radiation portal monitors at our nation's ports, including 181 radiation portal monitors at seaports. CBP also utilizes over 170 large-scale non-intrusive inspection devices to examine cargo and has issued 12,400 hand-held radiation detection devices to its CBP officers. The President's FY 2007 budget requests $157



million to secure current and next-generation detection equipment at our ports of entry through the DHS Domestic Nuclear Detection Office (DNDO). Over 600 canine detection teams, capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons, are deployed at our ports of entry. As reflected in the Radiation Portal Monitor Deployment at Seaports table, 621 RPMs will be deployed to our Nation's top seaports, which will allow us to screen approximately 98 percent of inbound containers by December 2007.

CBP's National Targeting Center (NTC) is also a critical component of our layered port security efforts. The NTC provides tactical targeting and analytical research support for CBP anti-terrorism efforts. Experts in passenger and cargo targeting at the NTC operate around the clock using tools like the Automated Targeting System (ATS) to identify tactical targets and support intra-departmental and inter-agency anti-terrorist operations. The ATS serves as the premier tool for performing transactional risk assessments and evaluating potential national security risks posed by cargo and passengers arriving by sea, air, truck, and rail. Using pre-arrival information and input from the intelligence community, this rules-based system identifies high-risk targets before they arrive in the United States. The Department's Science & Technology Directorate (S&T) is supporting the introduction of advanced intelligent algorithms to further improve these risk assessment capabilities.

A key responsibility of the NTC is the support that it provides to the field, including tactical targeting and research support for the CSI personnel stationed at critical foreign ports throughout the world. The NTC, combined with CSI, C-TPAT, the 24-hour rule, and ATS ensures that all containers on-board vessels destined for the United States are risk scored using all available information; and that all cargo determined to be of high risk are examined. The NTC, working closely with the Coast Guard, also vets and risk scores all cargo and cruise-ship passengers and crew prior to arrival. This ensures that DHS has full port security awareness for international maritime activity.

Further, DNDO's FY 2007 budget request of nearly $536 million, a 70% increase from FY 2006, includes $157 million that will allow for the acquisition and deployment of nearly 300 current and next-generation radiation detection systems at our ports of entry. These systems will be deployed and operated by CBP. In addition, DNDO's FY 2007 budget also includes $30.3 million for the development of enhanced cargo radiography screening systems for our ports of entry. These enhanced screening efforts will compliment the many information-based programs the Department already has in place for enhanced port security.

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

In order for the Department to increase its visibility into the security of our international supply chains, S&T is developing technology solutions that can be applied across the supply chain. Part of this effort is the development of a new class of security devices that will monitor the integrity of intermodal shipping containers and enable CBP Officers, CSI personnel and the NTC to gather information on the status of a container to improve risk assessment and data collection. When coupled with the broad supply chain security architectural framework currently under development by S&T, the Department will have the capability to bridge data and information between container security devices, shippers, and the National Targeting Center (NTC).

Finally, in addition to the work of the Coast Guard, CBP, S&T and the DNDO, the Port Security Grant program has awarded over $700 million to owners and operators of ports, terminals, U.S. inspected passenger vessels and ferries, as well as port authorities and State and local agencies to improve security for operators and passengers through physical security enhancements. The mission of the Port Security Grant program is to create a sustainable, risk-based effort for the protection of ports from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

The Preparedness Directorate will announce the application process for an additional $168 million in port security grants in the coming weeks, bringing total funding to over $870 million since 9/11. In addition, the FY 2007 President's Budget bolsters funding for infrastructure protection, including ports, through the $600 million Targeted Infrastructure Protection grant program. The FY 2007 request consolidates existing infrastructure grant programs into a single program with a 55 percent increase in funding.

With all of the layered efforts already in place, and the ongoing efforts that are supported in the 2007 budget request, port security has substantially improved since 9/11, and since the creation of the Department of Homeland Security.

DHS Legal Authority at the Ports

Congress has granted DHS legal authorities to take steps to ensure the security of America's ports and the cargo that passes through each of those ports.

Under the Magnuson Act, the Ports and Waterways Safety Act, and, most recently, the MTSA, the U.S. Coast Guard has authority to regulate security in all American ports. This includes the security for all facilities within a port, including terminal operators and vessels intending to call at a port or place subject to the jurisdiction of the U.S.

DHS Role in Cargo Security

The Administration recognized after September 11 that more was needed to protect the United States from terrorist attack, and it immediately identified the vulnerability posed by the millions of cargo containers entering our ports each year. DHS plays a primary

role in strengthening port and cargo security, and with the support of the Administration, we have made dramatic increases in these areas. Since September 11, funding for port and cargo security has increased by more than 700%, from $259 million in FY 2001 to $2.164 billion in FY 2004 and $2.183 billion in FY 2005. This upward trend continues with $2.455 billion for DHS port security allocated in FY 2006, and an additional 35% increase to $3.172 billion in the President's Budget request for FY 2007.

This money has helped implement a layered security strategy that pushes our security measures overseas. The reason is simple. The Federal Government realized after the 9/11 attacks that it would be far better to detect and interdict a threat to the United States when that container was thousands of miles away, rather than sitting in a U.S. port. So we pushed our borders out to do much more inspection and screening of cargo before it ever arrives at our shores.

The 24-Hour Rule and CSI

Our authority over shipping containers begins even before the container is loaded in a foreign port – and long before that container arrives in the United States. We require foreign companies to send us a list of the contents of a container 24 hours before the container is loaded on board the ship *in the foreign country.*

If CBP concludes that the contents of a particular container may be high risk, we can have it physically inspected or x-rayed in cooperating foreign ports.

This program, known as the Container Security Initiative (CSI), depends on the voluntary cooperation of foreign governments and foreign companies. We've gotten that cooperation around the world – including in Dubai, the United Arab Emirates.

Twenty-four hours before a ship is loaded, and therefore prior to departing the last foreign port for the United States, DHS receives a complete manifest of all the cargo that will be on that ship when it arrives in a U.S. port. This includes all cargo information at the bill of lading level, whether the cargo is destined for the U.S., or will remain on-board while in a U.S. port but destined for a foreign country. This rule applies to all containerized sea cargo whether departing from a CSI port or not.

Mandatory Advance Notice of Crew Members to DHS

Depending upon the length of the voyage, DHS receives additional notice concerning the crew of the vessel 24 to 96 hours before the vessel arrives in the United States. This is full biographic data identifying the crewmembers and passengers, if any, so that DHS can screen them against risk indicators, the terrorist watch list and other databases.

We also get information from the importer describing the declared value and manifest of the goods being imported.

Risk Analysis of Cargo and Crew

Thus, long before a cargo ship arrives at any U.S. port, DHS has the shipper's information, the ship's information, and usually the buyer's information about what is in the container. The data is compared to ensure that it matches, and is also compared against historical information to detect anomalous patterns.

This data is all scrutinized and processed through a complex program that runs against hundreds of risk indicators to assign the ship and its cargo a risk score. The crew and passengers are all vetted prior to arrival.

DHS has full information about the vessel, its contents, and the people on-board.

If DHS has a concern about the cargo, the Coast Guard and CBP meet and decide an appropriate course of action, which may include boarding the vessel at sea or at the entrance to the ship channel, or meeting the vessel dockside and immediately inspecting the suspect containers.

The Role of Terminal Operators like P&O and DP World

There has been a lot of attention in recent weeks about the potential threats posed by terminal operators. Let me first clarify what terminal operators do.

They do not run ports.

They certainly don't provide or oversee security for the entire port complex. That is the responsibility of the government and the local port authority, which is usually a government agency.

Terminal operators also do not obtain a comprehensive window into the breadth and depth of security measures that DHS employs to protect our ports and the cargo that enters those ports. The public fears that the DP World transaction have generated on this point are misplaced and lack a firm factual foundation, as I will explain later.

Terminal operators ordinarily sign a long-term lease for waterfront property in the port. They build a pier for ships, cranes to unload the ship, a parking lot to store the containers they unload, and perhaps a small management office. They make their money lifting containers out of ships and holding them for shippers.

That's what we're talking about here. Through its acquisition of P&O, DP World is hoping to take over the leases at twenty-four terminals in the United States. That's a relatively small part of the operations in the six ports where they would operate terminals, including New Orleans, Houston, Miami, Newark, Baltimore, and Philadelphia. Their filings indicate that DP World will also take over the P&O equities at other ports, but these consist of stevedoring and labor operations where P&O is not a designated terminal operator.

I understand from the Coast Guard that there are more than 800 regulated port facilities in the six ports where P&O operates terminals in the United States. So the twenty-four terminals in question here constitute less than 5% of the facilities in those six ports.

MTSA requires each terminal operator - because they operate inside the port – to file a facilities security plan with the Coast Guard that specifically details their compliance with all of the security measures required by federal law, including those enforced by the Coast Guard. The Coast Guard inspects the terminal and can check the terminal operator's plan at any time, and require more effective measures if the Coast Guard deems they are necessary.

These MTSA requirements for U.S. port security do not turn on the nationality of the terminal operator. U.S., British, Chinese, and UAE terminal operators are all subject to the same legal requirements, and the Coast Guard Captains of the Port can tailor each security plan to address the particular circumstances of each location.

What the Terminal Operator Knows about U.S. Security Measures

I noted earlier that ownership of a terminal operation does not give the terminal operator – foreign or domestic – a unique insight into the breadth and depth of DHS security measures nor provide a crafty terminal operator with ill intent access to inside information to avoid or evade DHS scrutiny.

The first time a terminal operator at a U.S. facility sees any of the law enforcement and security measures that DHS has in place concerning the vessel and cargo is when the ship arrives in the United States. Even then, all the terminal operator knows is that CBP has selected certain containers for examination. The operator is simply instructed to unload the containers, under DHS supervision, and deliver them to CBP for inspection. They are not told why.

CBP Examines 100% of Risky Containers

As I have noted already, CBP screens 100% of containers for risk. All containers that DHS determines to be of risk are examined using a variety of technologies. These technologies include: radiation screening, non-intrusive x-ray inspection, and as appropriate, physical examination.

This screening and examination is carried out by DHS employees tasked with the security of our seaports. They are assisted by longshoreman and stevedores in moving the containers, and by local law-enforcement authorities and port police to ensure the security of the port facilities.

All a terminal operator knows is that a container has been selected for examination, but not why the container was selected. The inspections and radiation detections are performed by CBP, not by the operator. Security is provided by a variety of government programs, agencies, and local law enforcement officials, not the terminal operator.

Special Measures to Detect Radioactive Devices

DHS component agencies and DHS' DNDO have worked closely with the Department of Energy to deploy radiation detection technology at domestic and foreign seaports. The Department of Energy is providing technical support to Dubai Customs to install four Radiation Portal Monitors in their main port in June. Some of this equipment is specifically dedicated to "in-transit cargo" passing through the Dubai port on its way to places like the U.S.

In the United States, we have deployed 181 radiation portal monitors at seaports to date, which allow us to scan 37 percent of arriving international cargo, and that number will continue to grow through the remainder of this year and 2007—again, allowing us by December 2007 to scan 98 percent of inbound cargo . CBP also has the ability to use portable devices to detect the presence of radiation at additional facilities, and CBP has issued over 12,000 hand-held devices to its officers with more on the way.

Since there is often confusion on this point, I want to restate it. CBP subjects 100% of all containers shipped to the United States to a risk assessment analysis and subjects 100% of any container over a certain risk threshold to further inspection.

In short, DHS already has a large number of measures in place relating to port and cargo security that are designed to ensure the security of our ports. These measures, and additional measures taken by local port authorities, greatly reduce the risks presented by the presence of any foreign terminal operator in a U.S. port.

The DP World CFIUS Case

As you know, I oversaw the DHS review of the CFIUS transaction involving DP World and P&O. Based on a thorough review, meetings with the company that began more than six weeks before the company filed for review, and the binding nature of an assurances agreement between DHS and the company to ensure security at U.S. ports, I stand fully behind the decision DHS made in January 2006 not to request further investigate this transaction.

Developments in the DP World Case

Nevertheless, DP World has announced that it is requesting an additional review by CFIUS. As noted by press reports, the company recently filed a second request for CFIUS review. DHS, as one of 12 CFIUS agencies, will be a full and active participant in that review and welcomes the opportunity to review the transaction anew. While we believe the 30-day review was rigorous and thorough, DHS will not prejudge its recommendation as a result of this 45-day investigation. DHS will also consider and investigate any additional steps the company proposes as part of its new notification or actions that it commits to taking, as well as any information provided by state or local officials or by members of Congress. As I explain in more detail below, DHS will once

again consult widely with its experts in the Department, including those at Coast Guard and Customs and Border Protection (CBP) who have primary responsibility for port and cargo security.

Before getting into the specifics of the DP World transaction, I would like to provide a general overview of DHS's participation in the CFIUS process.

Overview of DHS Participation in CFIUS

DHS is the newest member of CFIUS, added by Executive Order in 2003, after DHS was created. DHS has participated in the CFIUS process actively, and has placed a significant focus on nontraditional threats, as DHS has broad responsibility for protecting a wide variety of critical infrastructures.

CFIUS reviews dozens of transactions each year. In 2005, for example, CFIUS considered 65 discrete filings. DHS conducts a thorough review of each CFIUS case, and raises its concerns where issues arise.

The three most important questions DHS considers before deciding to seek an investigation are –

(1) Does DHS already have sufficient legal or regulatory authority to resolve any threat to homeland security that might be raised by the transaction?
(2) Does DHS have homeland security concerns about the parties or nature of the transaction?
(3) If DHS has homeland security concerns, can they be resolved with binding assurances from the parties to the transaction?

Only after answering these questions does DHS decide whether to seek an investigation in CFIUS. DHS examined those questions in the DP World case and, based on this careful assessment, made the judgment not to object to the transaction. All of the other 11 CFIUS member agencies conducted their own independent reviews of the transaction.

CFIUS Review of the DP World Transaction

DHS always examines the backgrounds of parties to a CFIUS transaction, and we did so in this case. DHS agencies – the Coast Guard and CBP -- had previously worked with both DP World and its management and found them to be cooperative and professional. Demonstrating this is the fact that DP World met with officials of DHS and DOJ on October 31 – more than six weeks before they filed on December 16 and our review began on December 17 – to provide confidential notice of their plans and begin answering questions.

DP World

DP World has played an invaluable role in the establishment of the first foreign-port screening program that the United States started in the Middle East. That's because

Dubai also volunteered to help in this innovative approach to security. DP World has voluntarily agreed to participate in screening of outbound cargo for nuclear material, and it has worked closely with CBP and the Dubai Customs Authority to target high-risk containers destined for the United States. These screening programs could not have been successfully implemented without the cooperation of Dubai Ports World.

P&O's Participation in the Customs-Trade Partnership Against Terrorism (C-TPAT)

British-based P&O, the owner of the U.S. facilities DP World is seeking to acquire, is and was a voluntary participant in CBP's Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the United States. DP World has committed to maintaining C-TPAT participation for all of the P&O ports subject to this acquisition.

C-TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

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

In Newark, New Jersey, all eight of the carriers who use P&Os Port Newark Container Terminal are also members of C-TPAT, which increases the overall security of the Newark facility.

The DP World CFIUS Transaction

As I previously noted, DHS considers three important questions in any CFIUS transaction: (1) does DHS already have sufficient legal or regulatory authority to resolve any threat to homeland security that might be raised by the transaction?; (2) does DHS have homeland security concerns about the parties or nature of the transaction?; and (3) if DHS has homeland security concerns, can they be resolved with binding assurances from the parties to the transaction?

I have addressed the first two of those questions, now let me turn to the third.

As part of its CFIUS review, DHS considers whether it should obtain any further commitments from the companies engaging in the transaction to protect homeland security. DHS has been aggressive in seeking such assurances as part of CFIUS reviews.

The assurances are carefully tailored to the particular industry and transaction, as well as the national security risks that we have identified.

The Assurances Agreements

DHS had never required an assurances agreement before in the context of a CFIUS review relating to a terminal operator or a port. But after analyzing the facts, DHS decided that we should ask for and obtain binding assurances from both companies to ensure that the companies would continue their record of cooperation with DHS.

The companies agreed after discussions to provide a number of assurances, two of which are particularly important.

First, both parties agreed that they would maintain their level of participation and cooperation with the voluntary security programs that they had already joined. This means that, for these companies, and these companies alone, what was previously voluntary is now mandatory.

In the U.S., the parties are committed to maintaining the best security practices set out in C-TPAT. In Dubai, the parties are committed to continued cooperation in the screening of containers bound for the U.S., including the radiation screening discussed above.

Second, the parties agreed to an open book policy in the United States. DHS is entitled to see any records the companies maintain about their operations in the United States -- without a subpoena and without a warrant. All DHS needs to provide to DP World is a written request and we can see it all. DHS can also see any records in the United States of efforts to control operations of the U.S. facilities from abroad.

Because C-TPAT requires a participating company to keep a current record of its employees, including Social Security Number and date of birth, this open-book assurance also allows us to obtain up-to-date lists of employees, including any new employees. DHS will have sufficient information about DP World employees to run the names against terrorist watch lists, to do background checks of our own, or to conduct other investigations as necessary.

These commitments were negotiated and obtained during the 30-day period the transaction was under CFIUS review, and DHS conditioned its non-objection to the transaction on an exchange of letters memorializing those commitments.

The Assurances Letters to DHS are Binding and Legally Enforceable

The assurances that DHS obtained from the companies are binding and legally enforceable, so that DHS and the U.S. Government could go into court to enforce them.

The companies also agreed in the assurances letters that DHS could reopen the case, which could lead to divestment by the foreign company if the representations the companies made to DHS turned out to be false or misleading.

DHS believes that DP World will adhere to both the letter and the spirit of the assurances letter, because the worst thing that can happen to a terminal operator's business is to lose the trust of the CBP officials who decide how much of that operator's cargo must be inspected every day. If we lose faith in the security and honesty of these parties, we will have to increase government scrutiny of the cargo they handle. That means more inspections and more delays for their customers.

And that is very bad for business.

That is why DHS is confident that the companies will work hard to continue to earn and retain our trust – and to fulfill their assurances – every day.

Conclusion

In short, after examining this transaction with care, DHS concluded that: (1) we have legal authority to regulate the U.S. security practices of these parties, including the ability to assess the maritime threat and intervene, at the foreign port of origin or on the high-seas, before potentially problematic cargo arrives at a U.S. port to be serviced by the parties; (2) DP World's track record in cooperating with DHS on security practices is already very good; and (3) DHS obtained assurances that provide additional protection against any possible future change in the cooperative spirit we have seen so far and that allow us to do further checks on our own.

Based on all those factors, DHS concluded that it would not object to the CFIUS transaction or seek an additional 45-day investigation.

I would be pleased to answer any questions that you have.

TESTIMONY OF GARY BROWN

INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

BEFORE THE

HOUSE SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

OVERSIGHT HEARING ON FOREIGN OPERATIONS AT U.S. PORT FACILITIES

MARCH 9, 2006

KWOPEIU29

COAST GUARD AND MARITIME TRANSPORTATION SUBCOMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES
OVERSIGHT HEARING ON
FOREIGN OPERATIONS OF U.S. PORT FACILITIES

MARCH 9, 2006

TESTIMONY OF GARY BROWN
ON BEHALF OF 60,000 MEMBERS OF
INTERNATIONAL LONGSHORE AND WAREHOUSE UNION (ILWU)

Chairman LoBiondo, Ranking Member Filner and members of the Committee, my name is Gary Brown. I am a third generation longshoreman at the Port of Tacoma, Washington, where I have worked for 37 years. I am also privileged to serve as the security liaison for the International Longshore and Warehouse Union. In this capacity, I have received numerous security certifications from the U.S. Coast Guard and FEMA and have successfully completed anti-terrorism training for the private sector, sponsored by the U.S. Attorney's office in Washington State.

On February 14 – 16, 2006, I organized a port security training session for ILWU members in conjunction with the Pacific Maritime Institute. Longshore workers from each of our Locals were trained on facility, company, and vessel security. We appreciate the first responders, Coast Guard, and Customs officials who made themselves available for this important training. Dock workers are literally on the front lines of our country's security and as such, must be aware of how to prevent and react to security incidents. The Union was obligated to initiate and pay for this training ourselves because our employer has failed to conduct the proper security training courses that Coast Guard regulations require.

We are at a critical time in the history of our country. The threat of a terrorist attack against the marine transportation system is the new reality. On March 14, 2004, suicide bombers, hiding in a metal cargo container, entered the Israeli port of Ashdod to commit terrorism. They killed 10 people and wounded another 16. All the victims were port workers, like me and other ILWU members.

As the tragedy in the Port of Ashdod has made chillingly clear, port security equates to worker safety in its most fundamental sense. Our lives and those in our port communities are literally on the line. In the event of a terrorist incident in an American port, the dockworker is the first one who is going to be killed or injured. Most dockworkers live within close proximity of the port and certainly within the impact-radius of any incident or explosion, be it chemical, biological or radioactive. We are talking about our families here, our children and our homes. It is in our own best interest to make sure American ports are secure; our family's lives and our livelihoods are at stake. Our commitment to port security is real, and it is not watered-down or diluted by cost or commercial concern. This, Mr. Chairman, brings me to the immediate issue at hand.

I. SUMMARY OF COMMENTS

The controversy over federal approval to permit Dubai Ports World, which is owned by a foreign government, to operate marine terminals at six East Coast ports is of the utmost importance for our country. The ILWU fully supports bipartisan calls in Congress for the Bush administration to direct the Committee on Foreign Investment in the United States (CFIUS) to conduct a full 45-day investigation of the Dubai contract. Although our seaports are part of the global economy, the ILWU believes that we should not rush to open the doors of such national assets to companies owned and operated by foreign governments where serious concerns exist regarding terrorist activities and funding. We, therefore, urge that the decision for approval be based on the national security interests of the United States rather than the commercial interests of any one company or country.

But we also urge the federal government, including Congress, to focus its attention beyond the controversy over one future, commercial contract and to recognize and correct the immediate, major deficiencies of security that exist today in America's ports. It is the current lack of effective port security since the terrorist attacks of 9-11 that is the real concern of dockworkers and millions of Americans who live in close proximity to our nation's ports.

The Maritime Transportation Security Act (MTSA), initiated by this Committee and passed in 2002, provides the foundation for the nation's port and cargo security. In 2004, the Coast Guard -- designated as the lead enforcement agency under MTSA -- issued comprehensive, detailed and - we believe - effective port security regulations for marine terminal and vessel operators to follow. Unfortunately, the MTSA security regulations have been implemented and honored in the breach, with both foreign and domestic companies ignoring most of the required measures designed to improve port security. Just like the current case over the Dubai contract, the problem of system wide noncompliance with existing port security regulations arises from allowing commercial interests to override security interests.

MTSA regulations allow terminal operators to write their own facility security plans. This is a mistake and yet another example of commercial interests overriding security concerns. We allow terminal operators to create their own security rather than having one model and enforcement mechanism for all terminals at all ports.

The ongoing security crisis in our ports also stems from the lack of funding, training, and infrastructure. The overarching problem we now face is making the enforcement mechanism effective and capable of ensuring that essential port security measures mandated by Congress are fully implemented. However, the Coast Guard is a waterside and vessel enforcement specialist. They are not a "landside" or "terminal" enforcer of container terminal regulations and operations. What is going to be the USCG's defined enforcement role and how is it going to differ from the past? How is the USCG going to "force" terminal operators to conform? What is going to be the compliance trigger if and when terminal operators are found to be non-compliant? Most importantly, who is going to create the procedures and protocols to instruct the Coast Guard in the basics of terminal operations? Effective port security regulation compliance will require a comprehensive, fully funded, land-side compliance program employing large numbers of Coast Guard personnel who must be trained in terminal container operations and complex information systems format. This is a complex industry,

and the volumes are astronomical.

In conclusion, the ILWU believes that the debate over Dubai will do little to protect America's seaports unless the federal government takes this opportunity to recognize and correct the glaring, major defects in port security that exist today.

In our written testimony, we have laid out specific security protocols at marine terminals that must be followed to ensure real port security. I look forward to answering questions about these recommendations.

Thank you.

ILWU RECOMMENDATIONS FOR MARINE TERMINAL SECURITY

Security mandates may impose significant and additional operating costs on the maritime industry. However, port facility operators have repeatedly refused requests to implement some of the following, all of which are mandated by the Coast Guard regulations, because of cost and/or commercial concern:

1. Access control procedures for the positive identification of people, vehicles and cargo before entering a port facility must be immediately implemented as required by regulation 33 CFR ' 105.255(a), (e)-(g), and105.265 (a)-(d).

   Presently, truck drivers are the largest single occupational group working within the terminals. **Access is granted with little authentication of identity and virtually no inspection** of their "sleeper cabs," which frequently house friends and family. Ironically, these drivers, once inside the terminals, have unlimited access to all areas of the terminals without oversight or supervision. Any of the fourteen terminals in the Ports of LA/Long Beach may have hundreds of drivers on each of the terminals at any one time.

2. Proper documentation, placarding and separation of all dangerous cargo and hazardous material must be performed as required by regulation 33 CFR ' 105.265(a)(9).

   Presently, **hazardous cargo is frequently unmarked** and integrated with other cargo.

3. The integrity and correctness of all seals on containers must be checked as they enter a port facility and as they are placed in inventory on the docks to detect and deter any tampering, as required by regulation 33 CFR ' 105.265(b)(4) and 105.265(c)(4).

   Presently, this is not being done at most port facilities. In fact, since September 11, many facility operators have discontinued past practice of checking these seals.

   Many terminal operators have implemented remote camera technology at our gates that have replaced the physical and visual inspections of seals. However, the **resolution of the camera is too low to determine whether a seal has been tampered with** or even to read the number on the seal.

4. All port workers must be trained as to the basic requirements of the port facility security plan, the detection of security problems and, most importantly, the proper response and evacuation procedures during a security incident as required by regulation 33 CFR ' 105.215.

   As of today, **port facility operators refuse to share with dockworkers any parts of their security plans** on grounds of "confidentiality";

dockworkers cannot protect themselves or our ports if they are excluded from security initiatives. The ILWU would appreciate any grant money that can be made available to the union for training, in light of our employer's failure to cooperate.

5. Complete documentation of cargo must be confirmed before entering a facility as required by regulation 33 CFR ' 105.255(e)(1), (3).

   Presently, cargo is received with missing or incomplete documentation; but the cargo is allowed to enter with a STC (Said To Contain) designation or with the ambiguous "Dummy" which often means there will be **NO LISTING OF CONTENTS AT ALL.** This container is allowed to be "entered" into the facility without ever knowing what is inside.

Most of the deficiencies in port security can be corrected through continuous and rigorous enforcement of and adequate funding for the Coast Guard regulations. In this regard, we applaud the introduction of Senate Bill 1052, the Transportation Security Improvement Act (TSIA), which would improve the examination of cargo shipments overseas before they reach U.S. shores, provide procedures for the speedy resumption of commerce in the event of a seaport attack, and expanded the use of inter-agency operations centers (IOCs).

However, there are at least two additional security measures, not specifically covered in the existing or proposed regulations that should be immediately implemented in order to protect our ports.

- **EMPTY CONTAINERS**: The inspection of all containers marked as "empty" upon entering a port facility is a no-brainer. On any given day, as much as forty percent of the containers delivered into West Coast ports consist of "empty" containers. Many facility operators presently receive and process "empty" containers without confirming that they are truly empty. Containers marked as **empty** provide a golden opportunity. The good news is that unlike containers filled with cargo, the inspection of empty containers is quick and easy. It is a relatively cheap and painless way of confirming the absence of a dangerous substance or device, and the absence of persons illegally attempting to gain access. This, of course, makes the inspection of "empty" containers all the more compelling and an absolute necessity in any port security program.

  There have been assertions made by industry officials that all West Coast terminal operators are inspecting empty containers. This is simply not true. The ILWU has furnished the Coast Guard with formal letters from both stevedores and terminal operators informing the union that, at certain facilities, empty containers will no longer be inspected.

- **24 ADVANCE NOTICE OF EXPORT CARGO:** Requiring the proper documentation of export cargo 24 hours in advance of its receipt at the port facility is logical and follows the rule for import cargo. While U.S. Customs requires twenty-four-hour advance notice of the contents of all containers arriving aboard vessels, *see* 19 CFR ' 4.7(b), current federal regulations require no comparable notice for export containers arriving by truck or

rail. Imposing a 24-hour detailed notice rule on inbound cargo, but not trucks or trains delivering "outbound export cargo" into the terminals makes little sense.

Requiring such notice would provide facility personnel additional time to spot errors relating to the misidentification of cargo, fix the honest mistakes, and determine what containers require further inspection. It would also lead carriers to spot more unidentified HazMat materials before they are transported.

It is important to understand that while "empty" containers and export cargo are ultimately destined for other countries, they also pose immediate security risks for our seaports and the country. This is a national security issue for two reasons:

1. Once the cargo within the container has been unloaded at its eventual destination, there is no system, protocol, or requirement in place making the last shipper responsible for closing and sealing the doors. As a result, this empty container will travel over-the-roads of the U.S. unlocked and open. It may serve as a platform or vehicle for anything or anyone who may desire to do harm to our country. It may lie unattended on city streets or even within the port for days or even weeks until it is returned to the terminal for shipment (usually back to Asia.) Who knows what has been stored or smuggled inside? Who knows what kind of plan someone may come up with utilizing this empty container?

2. Once loaded onto a vessel, empty containers travel with that vessel between and among U.S. ports until they are eventually off-loaded, whether in a foreign port, or still here in the U.S. At any point along the vessel route, a weapon of mass destruction, planted inside an "empty" container or among export cargo, could be later detonated at the next American port-of-call. The Al-Quaeda terrorists executed their September 11 attacks from within the United States. The same strategy may well be used again and should be anticipated. Prevention with respect to cargo and containers in our marine transportation system depends on a thorough knowledge of containers and cargo handling methods and operations. The 9/11 terrorists exhibited an amazing ability to gather intelligence, and then plan, fund and execute a successful operation. The defense of our country demands no less.

Statement of Dr. James Jay Carafano
Senior Research Fellow
The Heritage Foundation

Before the House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation

Mr. Chairman and other distinguished Members, I am honored to testify before you today.[1] In my testimony, I would like to (1) emphasize why secure ports are essential to the nation; (2) describe the significant security threats the U.S. faces today and in the future; and (3) propose steps that Congress take to improve the security of foreign-owned maritime infrastructure including revisions to the Maritime and Trade Security Act.

Maritime Security Matters

Maritime trade is vital to the U.S. economy. Almost one-third of the U.S. gross domestic product (GDP) is derived from trade. As you know, 95 percent of American overseas trade traffics the maritime domain. According to the American Association of Port Authorities, $1.3 billion worth of U.S. goods move in and out of U.S. ports every day. In addition, many major urban centers (more than half of the U.S. population) and significant critical infrastructure are in proximity to U.S. ports or are accessible by waterways.[2]

---

[1] The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2005, it had more than 275,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2005 income came from the following sources:

Individuals	63%
Foundations	21%
Corporations	4%
Investment Income	9%
Publication Sales and Other	3%

The top five corporate givers provided The Heritage Foundation with 2% of its 2005 income. The Heritage Foundation's books are audited annually by the national accounting firm of Deloitte & Touche. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

[2] Maritime security also has a critical defense dimension. The vast majority of U.S. military forces and supplies projected overseas transit through U.S. ports. In fiscal year 2003 alone, for example, the U.S. Military Traffic Management Command shipped over 1.6 million tons of cargo in support of Operation Iraqi Freedom. Most military supplies and hardware move through only 17 seaports. Only four of these ports are designated specifically for the shipment of arms, ammunition, and military units through Department of Defense (DOD)-owned facilities. For an overview of the military's reliance on ports and associated security risks, see U.S. General Accounting Office, "Combating Terrorism: Preliminary

Ports can also be tempting for terrorists. As points of entry and exit, they are critical nodes that affect terrorist travel and transiting of material support or weapons. They might also be prime targets for terrorist strikes. The economic, physical, and psychological damage that would result from a significant terrorist attack targeting maritime commerce or exploiting America's vulnerability to sea strikes is difficult to estimate, but the stakes are high. A significant breakdown in the maritime transport system would send shockwaves throughout the world economy. In fact, in a worst-case scenario, a large attack could cause the entire global trading system to halt as governments scramble to recover. Drastic and inefficient solutions could also be put in place, such as the complete closure of some ports and duplicative and lengthy cargo checks in both originating and receiving ports.[3]

During the next decades, maritime commerce likely will become an even larger and more important component of the global economy. The future maritime system will be robust, yet fragile. Maritime shippers increasingly concentrate their traffic through major cargo hubs ("mega-ports") because of their superior infrastructure. In the United States, 50 ports account for approximately 90 percent of all cargo tonnage.[4] Their specialized equipment is essential for the loading and off-loading of container ships, which constitute a growing segment of maritime commerce. Today, U.S. seaports unload approximately 8 million loaded containers annually.[5] Analysts forecast the volume of global container traffic will double over the next 20 years.[6] The rising use of container shipping and mega-ports has lowered the costs and improved the reliability of maritime commerce, leading firms to rely increasingly on rolling inventories and just-in-time deliveries. These trends have produced significant economic benefits for many industries engaged in international commerce, but have also made individual companies in the supply chain more vulnerable to interruptions.[7]

Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports," GAO-02-955TNI, July 23, 2002. See also U.S. General Accounting Office, "Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments Through Domestic Seaports," GAO-03-15, October 2002, pp. 5–10.

[3]A preliminary estimate in 2003 placed this cost at tens of billions of dollars, nearly $60 billion for the U.S. alone. Organisation for Economic Co-operation and Development, "Directorate for Science and Technology and Industry, Maritime Transport Committee, Risk Factors and Economic Impact," July 2003, at *www.oecd.org/dataoecd/19/61/18521672.pdf* (October 29, 2004).

[4]U.S. Congress, House of Representatives, "Maritime Transportation Security Act of 2002," Conference Report, 107–777, p. 4.

[5]"Marine Insurers Contemplate Increased Security Regulations," *Claims Magazine,* December 2003, p. 12.

[6]William G. Schubert, Maritime Administrator, Department of Transportation, Testimony before the Committee on The Judiciary, Hearings on the Security of our Seaports, February 26, 2002, at *http://usinfo.state.gov/topical/pol/terror/02022701.htm.* (February 27, 2005)

[7]For a comprehensive discussion of these vulnerabilities, see Daniel Y. Coulter, "Globalization of Maritime Commerce: The Rise of Hub Ports," in *Globalization and Maritime Power*, edited by Sam J. Tangredi (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 2002), pp. 133–142.

Qualifying Maritime Threats

A special report prepared by the Maritime Security Working Group (chaired by The Heritage Foundation) was asked to address the long-term security threats to the United States in the maritime domain.[8] The group—consisting of experts from academia, research centers, the private sector, and government—concluded the major trends that will affect U.S. maritime security are:

- *Internal Threats from Rogue Actors.* The greatest vulnerability to maritime infrastructure may be internal threats, i.e., employees who have an intimate knowledge of operations and facilities and access to transportation and port assets.

- *The Growth of Maritime Criminal Activity.* Piracy, human trafficking, and drug smuggling will continue. Terrorists could mimic or partner with criminal enterprises.

- *The Lack of Visibility in Non-Commercial Maritime Activity.* Currently the United States lacks sufficient means to monitor maritime activity. Terrorists could capitalize on this failing in many ways, including mines and other underwater attacks, smuggling by private craft with small payloads delivered outside ports, or attacks by small craft.

- *The Maritime Domain as a Target and Facilitator of Threats against the Environment.* Opportunities for infectious diseases and other environmental threats carried by seaborne traffic will increase with greater maritime commerce.

- *Anti-Access Strategies a Real Possibility.* An enemy might attack vulnerable targets on U.S. territory as a means to coerce, deter, or defeat the United States.

- *Stand-Off Attacks from the Sea.* State and non-state groups will be capable of mounting short-range ballistic missiles and cruise missile attacks—possibly employing weapons of mass destruction—from U.S. waters.

The group found the challenges identified above as enduring, disturbing, and inadequately addressed.

Misplaced Maritime Priorities

On the other hand, the group found that there were other threat scenarios that are often discussed as less plausible or that post-September 11 security regimes have made less likely. In particular, since 9/11, some security analysts argue that every container bound

[8]James Jay Carafano, and Alane Kochems, eds. "Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism," Heritage *Special Report* No. 3, February 17, 2005, at *www.heritage.org/Research/HomelandDefense/sr03.cfm.*

for the United States should be inspected because one could possibly be used to smuggle a nuclear weapon or a "dirty" bomb (radiological dispersion device) into the country. To counter this threat, they propose spending billions of dollars on container and port security.

This argument fails on four counts. (1) The nuke-in-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, a private watercraft would be a safer and more secure way to transport the weapon, either directly to the target (e.g., a port) or indirectly by landing it in Mexico and then driving it across the border. (2) While nuclear smuggling is possible, so are dozens of other attack scenarios. It is dangerously myopic to over-invest in countering one tactic when terrorists could easily employ another tactic. (3) Searching every container and hardening every port is an extremely inefficient and expensive way to stop terrorists from using cargo containers. (4) There is no apparent viable business case for many of the proposed solutions for "hardening" shipping containers or conducting 100 percent physical container inspections. These measures would provide only minimal utility at the cost of billions of dollars in new duties, taxes, and operating costs.

As a matter of common sense, the United States should not attempt to make every cargo container and port into a miniature Fort Knox. Securing trade requires a more comprehensive and effective approach than just putting up fences and gates, posting guards at ports, and inspecting all cargo containers as they enter the country. This approach fails on two counts: (1) It wastes security resources by inspecting things that are not a security risk. (2) It creates isolated, easily bypassed chokepoints to address specific (and unlikely) threats.

Efforts to protect trade should focus on improving security of the entire supply chain. Strengthening the U.S. maritime security regime is a good place to start.

Making the Seas Safer

The Heritage Foundation's maritime security working group has identified several areas that should be the centerpiece of U.S. effort to help secure the maritime enterprise. In addition to strengthening current programs,[9] the three most critical additional enablers to current efforts should be:

- *Fix the Coast Guard First.* U.S. Coast Guard operations are central to virtually every aspect of maritime security from enforcing ISPS to interdicting suspect

[9] See, Alane Kochems, "GreenLane Maritime Cargo Security Act: A Good First Attempt," January 26, 2006, Executive Memorandum #989, at *www.heritage.org/Research/HomelandDefense/em989.cfm.*

cargo under the Proliferation Security Initiative. Fully funding the Coast Guard's modernization program, Deepwater, at $1.5 billion per year is essential.[10]

- *Enhance Public-Private Information Sharing.* In particular, better commercial data must be submitted to the Automated Targeting System (ATS) that would facilitate higher quality risk assessments of cargo in the pre-vessel-loading security screening process. This data could include: better cargo descriptions; identification of seller and purchaser; the goods point of origin; country from which goods are exported; ultimate consignee; exporter representative and name of broker; and origin of container shipment.

- *Improve International Cooperation.* The U.S. National Security Strategy rightly calls for encouraging economic development through free markets and free trade and enhancing the capacity of developing nations to compete in a global economy. Concurrently, however, the United States is also rightly promoting international security regimes designed to prevent terrorists from attacking or exploiting global trade networks. Meeting these requirements is difficult not for the Dubai's of the world, but for developing countries that lack mature infrastructure, robust human capital programs, and adequate financing. Federal agencies have disparate programs to assist these countries in enhancing their maritime security. These programs are not synchronized with each other or with our allies in Europe or Asia. Congress should begin to address this issue by require the General Accountability Office to inventory and assess the effectiveness of the various U.S. program and their international counterparts.[11]

In addition to these efforts, the Congress should take appropriate measures to address concerns over foreign-owned maritime infrastructure in the United States.

Assuring Surety in Foreign-Owned Infrastructure

The sale of a British-based company which controls cargo handling operations at number of U.S. facilities—including six major U.S. ports—to Dubai World Ports, a government-owned company in the United Arab Emirates, has raised many concerns. While a review of the facts suggests no apparent security issues,[12] these concerns do reflect the importance of ensuring that the U.S. government has undertaken all reasonable efforts to make the seas safer.

---

[10] Statement of Dr. James Jay Carafano, Senior Research Fellow, The Heritage Foundation, Before the Senate Committee on Commerce, Science, and Transportation, March 24, 2004, at *www.heritage.org/Research/HomelandDefense/tst032404a.cfm#_ftn2.*

[11] James Jay Carafano, and Ha Nguyen, "Homeland Security and Emerging Economies," Heritage Backgrounder #1795, September, 14, 2004, *at www.heritage.org/Research/HomelandDefense/bg1795.cfm*

[12] James Jay Carafano and Alane Kochems, "Security and the Sale of Port Facilities: Facts and Recommendations," WebMemo #997, February 22, 2006, at *www.heritage.org/Research/HomelandDefense/wm997.cfm.*

The Maritime Transportation and Security of Act (MTSA) of 2002 did not consider the sale of maritime infrastructure to or between foreign-owned firms operating at U.S. ports. Congress might well consider what revisions to this law might be appropriate. These could include require:

- The company facility security officers at U.S. ports to be U.S. citizens, successfully complete a suitable background investigation, and be qualified to receive a transportation worker identification credential (TWIC);
- A mandatory review of the company security plan by the U.S. Coast Guard prior to the transfer of ownership;
- Notice after the transfer of ownership of any proposed material changes to the security plan, as well as committing to meet with U.S. officials to review changes prior to implementation; providing relevant information required to evaluate the changes; and addressing security concerns before the changes are implemented;
- Committing to reasonable steps to assist and support any federal, state, or local law enforcement agencies in conducting law enforcement activities related to facilities or services provided by the company in the United States;
- Disclosing information on the design, maintenance, or operation of U.S. facilities or operations as they relate to a law enforcement investigations;
- Providing any relevant records in the United States involving matters relating to foreign operations of the company that relate to a law enforcement investigation;
- Committing to participation in the Customs–Trade Partnership Against Terrorism (C–TPAT); [13]
- Establishing penalties for non-compliance with the above measures;
- Applying these requirements to any transfer of critical maritime infrastructure whether the gaining company is U.S. or foreign-based; and
- Requiring that major U.S. seaports establish intelligence and information-sharing fusion centers (Joint Operations Center) similar to the pilot-project Seahawk at the port of Charleston, South Carolina, and requiring that the centers be funded equitably and jointly by all public and private stakeholders at the port.

Port facilities are just one of many aspects that should be considered in developing a comprehensive maritime security regime. The United States should approach cargo and port security from the perspective of a complex global system rather than attempting (and failing) to make ports and containers impervious to terrorist threats. Ports are just one part of a system, designed to move people and things quickly in immense volumes.

---

[13] The Customs–Trade Partnership Against Terrorism (C–TPAT), another CBP program, allows companies that have taken voluntary steps to secure their containers and supply chains to move more quickly through the inspection process and undergo fewer inspections. This program gives companies incentives to tighten their supply-chain practices, improving overall security. It creates a win-win situation for both U.S. trade security and the companies that comply. See, U.S. Customs and Border Protection, "Securing the Global Supply Chain," at *www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf.*

The best way to secure a port is to keep bad things and bad people out of the port to begin with. And that means securing the system, not the port. Modifications to MTSA, such as those proposed here, should be designed to make port security an integral and useful component to securing the maritime domain—and not a misguided attempt to turn America's ports into mini-Maginot lines.

Winning the Long War

President George W. Bush was right to suggest that we are engaged in a long war in his State of the Union Address. It is an important distinction. Protracted conflicts like the Cold War or the War on Global Terrorism require different kinds of strategies—strategies that place as much emphasis on sustaining the capacity of the state to compete over the long term as they do on diminishing the enemy.

Good long war strategy requires meets four equally compelling priorities: (1) providing security; (2) promoting economic growth; (3) safeguarding liberties; and (4) winning the war of ideas. Each has relevance to the maritime domain.[14] This Committee and Congress need to insist that the Bush Administration implement measures to meet each of these priorities, not trading one off for another. This criterion should serve in evaluating *any* security issue, including protecting America's maritime infrastructure in the United States

Thank you again for the opportunity to address this vital question.

[14]James Jay Carafano and Paul Rosenzweig, *Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom* (Washington, D.C.: The Heritage Foundation, 2005).

THE HONORABLE BOB FILNER
RANKING DEMOCRAT
SUBCOMMITTEE ON COAST GUARD AND
MARITIME TRANSPORTATION
OVERSIGHT HEARING ON
PORT AND MARITIME SECURITY
March 9, 2006

Thank you Mr. Chairman for scheduling today's hearing on port and maritime transportation security. Port security has received more publicity in the past month than any time in the past decade.

While foreign-control of critical U.S. infrastructure should be thoroughly reviewed before it is approved, there are other maritime transportation security weaknesses that may pose an even greater threat to the security of the United States.

The Maritime Transportation Security Act of 2002 (MTSA – pronounced MITSA) required the Secretary of Homeland Security to establish "secure systems of transportation" to provide security standards for the stuffing and transportation of containers to the United States. To date nothing has been done to implement and enforce meaningful security standards for containers from the point that the container is stuffed until it is delivered to an inland city in the United States.

The MTSA required the Secretary of Homeland Security to develop standards for seals and locks on containers so that if a container is breached and a Weapon of Mass Destruction (WMD) is inserted while it is on a rail siding in some country – we would know about it. To date, no such standards have been prescribed. Containers enter the U.S. every day with a simple plastic seal – that could have been replaced somewhere along the transit without anyone knowing.

The concept behind MTSA was to "push the borders out" – by the time a container enters the U.S. with a WMD – it is too late. We need to scan 100% of the

containers overseas before they are loaded on the ship destined for the U.S. To date, very few containers are scanned before they are loaded on a ship.

MTSA required the Secretary of Homeland Security to conduct background checks on those individuals that have access to the secure areas of a marine terminal in the U.S. to make sure they don't pose a terrorism security risk. To date, over 3 years after MTSA was signed into law, no background checks have been conducted.

MTSA required the Secretary of Homeland Security to restrict entry to secure areas of marine terminals to individuals that have biometric identification cards to ensure that they are who they say they are. To date, no standards have been published for ports and marine terminal operators to implement.

Mr. Chairman, we may have more closed circuit TV's on our marine terminals than we did when MTSA was enacted – but that's only going to help prevent theft and pilferage of cargoes in the U.S.

If we think we have implemented security standards to prevent a WMD from entering the United States – we're fooling ourselves and the American people.

As the Coast Guard testified in a hearing last year, they are only interdicting 15% of the drugs entering the United States by water every year. I find that outrageous – particularly since we know that almost all of these drugs are coming from Columbia. How do we expect to secure our borders from a WMD – when we can't even stop cocaine?

Thank you Mr. Chairman scheduling this very important hearing. I look forward to working with you to improve the security of our nation's maritime transportation system.

COUNCIL ON FOREIGN RELATIONS

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

"The Continued Vulnerability of the Global Maritime Transportation System"

Written Testimony before

a hearing of the

Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
United States House of Representatives

on

"Foreign Operations of U.S. Port Facilities"

by

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

Room 2165
Rayburn House Office Building
Washington, D.C.

9:30 a.m.
March 9, 2006

"The Continued Vulnerability of the Global Maritime Transportation System"

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

Chairman Lobiondo, Ranking Member Filner, and distinguished members of the House Subcommittee on Coast Guard and Maritime Transportation. Thank you for inviting me this morning to discuss the federal government's progress in implementing maritime security measures as required by the Maritime Transportation Security Act of 2002 and my recommendations of how to advance this critical agenda.

The controversy surrounding the takeover of five American container terminals by Dubai Ports World has had the salutary benefit of engaging Washington and the American people in a national conversation on the state of port security. This is long overdue given the enormous national security and economic security stakes should the next catastrophic terrorist attack on U.S. soil involve the global maritime transportation system and America's waterfront. While it has too often been lonely work, Chairman Lobiondo, I commend you and your committee for your leadership in advocating that our critical maritime infrastructure should not be overlooked in our post-9/11 efforts to secure the American homeland.

This is my second opportunity to appear before this committee. On August 25, 2004, I provided testimony that I entitled "The Ongoing Neglect of Maritime Transportation Security." At the hearing I said: "I believe maritime transportation is one of our nation's most serious vulnerabilities, and we are simply not doing enough to respond to the terrorist threat to this critical sector." Sadly, I have seen too little progress in the ensuing 18 months to modify that assessment. Based on my visits to a dozen major seaports within the United States and abroad since 9/11, my conclusion is that the security measures that are currently in place do not provide an effective deterrent for a determined terrorist organization intent on exploiting or targeting the maritime transportation system to strike at the United States.

At the federal level, the primary frontline agencies—the Coast Guard and Customs and Border Protection Agency—are grossly under-funded for what became essentially a new major mission for them on 9/11. On the local and state levels, the size of port authority police forces remain tiny, providing often only token police presence within most seaports. While the Maritime Transportation Security Act of 2002 represented a constructive stepping off point for advancing security within this sector, we have made little meaningful progress since then.

In my remarks today, I will speak to both the shortfalls in our port security efforts within the United States and with our efforts to advance port security overseas and provide some recommendations on how we should proceed. Our domestic and international efforts must be complementary because seaports, at the end of the day, are simply onramps and offramps into a global transportation network. To focus on just the security of U.S.

seaports is a bit like a computer network security manager who only puts in place firewalls for the computers within reach of his desk. If the whole network is not secure, such an effort will be futile.

To begin with, we must candidly acknowledge that MTSA is more of a sketch than a security blueprint; that is, it sets forth general requirements without establishing minimum standards for satisfying those requirements. For instance, the MTSA requires vessels and marine facilities have a plan for establishing and maintaining physical security, passenger and cargo security, and personnel security. However it does not define what that security is. It requires that there be a system for establishing and controlling access to secure areas of the vessel or facility, but does not elaborate how that should be done. It mandates that there be procedural security policies, but provides no guidance on what those policies should be. MTSA requires that there be a "qualified individual" to implement security actions, but sets no standards on what it takes to be "qualified." There are not even any minimal training standards. The Coast Guard has worked with the Maritime Administration to create a "model" training course, but there is no requirement that facility or ship security officers attend a certified course base on this model curriculum.

The International Maritime Organization's International Ship and Port Facility Security code (ISPS) mirrors the MTSA in that it provides a framework of requirements without stipulating specific standards for satisfying those requirements. Ships and port facilities must have security plans, security officers, and certain security equipment but the code leaves it up to each foreign government to provide the specifics. There are no minimum training standards for becoming a "qualified" security officer. There are no mandatory guidelines for what constitutes perimeter security. There are no mandated requirements to govern facility access controls. It is also important to point out that while most ships are in the business of moving cargo, the ISPS code does not address cargo security.

When it comes to port security, the buck essentially stops outside Washington, DC. Since seaports in the United States are locally run operations where port authorities typically play the role of landlord, issuing long-term leases to private companies; it falls largely to those companies to provide for the security of the property they lease.

In the case of Los Angeles, this translates to the security for 7500 acres of facilities that run along 49 miles of waterfront being provided for by minimum-wage private security guards and a tiny port police force of under 100 officers. The situation in Long Beach is even worse with only 12 full-time police officers assigned to its 3000 acres of facilities and a small cadre of private guards provided by the port authority and its tenants. The command and control equipment to support a new joint operations center for the few local, state, and federal law enforcement authorities that are assigned to the port will not be in place until 2008. Up to 11,000 independent truck operators have access to the port terminals yet there still is no credentialing system in place to confirm the backgrounds of the drivers. West Coast terminal operators have no way of identifying who is in their facilities at any given moment. In the four years since September 11, 2001, the two cities have received less than $40 million in federal grants to improve the port's physical

security measures. That amount is equivalent to what American taxpayers spend in a single day on domestic airport security.

But the fallout from a terrorist attack on any one of the nation's major commercial seaports would hardly be a local matter. For instance, should al Qaeda or one of its imitator organizations succeed in sinking a large ship in the Long Beach channel, the auto-dependent southern California will literally run out of gas within two weeks. This is because, as Hurricanes Katrina and Rita highlighted, U.S petroleum refineries, are operating at full throttle and their products are consumed almost as quickly as they are made. If the crude oil shipments stop, so too do the refineries and there is no excess capacity or refines fuels to cope with a long term disruption.

But the most serious consequence of a major terrorist attack on America's waterfront is if it involved a weapon of mass destruction smuggled into one of the over nine million 40' cargo containers that entered U.S. seaports in 2005. The September 11, 2001 attacks on New York and Washington, the March 11, 2004 attacks on Madrid, and the July 7, 2005 attacks on London highlight that transport systems have become among the most favored targets for terrorist organizations. Cargo containers have long been exploited to smuggle narcotics, migrants, and stolen property including luxury automobiles. Their vulnerability is highlighted by the billions of dollars in cargo losses derived from theft each year. A typical cargo container that is shipped from Asia will pass through over a dozen transportation waypoints before it is loaded on a ship destined for the United States. Most are "secured" only with a fifty-cent lead seal passed through the pad-eyes on the container doors.

It is just a question of time before terrorists with potentially more destructive weapons breach the superficial security measures that have been put in place to protect the ports, the ships, and the millions of intermodal containers that link global producers to consumers. Should that breach involve a "dirty bomb," the United States and other states will likely raise the port security alert system to its highest level while investigators sort out what happened and establish whether or not a follow-on attack is likely. Multiple port closures in the United States and elsewhere would quickly throw this system into chaos. Container ships already destined for the United States would be stuck in anchorages unable to unload their cargo. Ships would be delayed in overseas loading ports as the maritime industry and their customers try to sort out how to redirect cargo. Marine terminals would have to close their gates to all incoming containers since they would have no place to store them. Trucks and trains would be stuck outside the terminal with no place to go. If they are carrying perishable goods, the cargo would perish. Also, the trucks and trains would not be able to re-circulate to pick up new shipments until they can get rid of the old ones. Goods for export would pile at factory loading docks with no place to go. Imports to support "just-in-time" deliveries would be no shows and soon factories would be idled and retailers' shelves would go bare.

In short, a catastrophic terrorist event involving the intermodal transportation system could well lead to unprecedented disruption to the global trade system. In economic terms, the costs associated with managing the attack's aftermath will substantially dwarf

the actual destruction from the terrorist event itself. Those costs will be borne internationally which is why transportation and trade security must be not only a U.S. Homeland Security priority, but an urgent global priority.

As grave as this threat is, in our fifth year since the 9/11 attacks, there still are no minimum federal standards for access control, perimeter control, electronic surveillance, guards, and communications. State and local port authorities have not been able to make any significant progress towards improving the state of security within their ports. This is largely because ports face a competitive environment where they must make significant capital investments to improve the commercial operations in order to retain or attract shipping lines. It they divert funds away from capital improvements to pay for added security they may face a decline in vessel traffic that reduces their revenues. If they try to pass along increase security costs to their private tenets, those tenets may decide to move to a lower cost neighboring port. In short, in the absence of a level national playing field, U.S. port authorities have been reluctant to make major new investments in security.

The MTSA mandates that ships approaching U.S. waters be equipped with an Automatic Identification System (AIS). However the system the Coast Guard is putting in place is largely a line-of-sight system with a range of about 20 miles. This provides very little time to respond before the ship is detected. Since it is unlikely that Coast Guard patrol vessels would be routinely be available to respond to the arrival of a rogue vessel, that vessel could inflict substantial harm long before the means could be mustered to forcibly stop it.

The Coast Guard has in place a requirement that all vessels approaching U.S. ports provide notification of the vessels last five ports of call, its cargo, and crew members 96 hours before arrival. But it is essentially an honor system since the Coast Guard has no way of confirming when a vessel is 96 hours away, if it is accurately reporting its ports of call and cargo, or if it does not leave any names off its crew list.

At the port of loading, a port facility is supposed to be operating in compliance with the ISPS code. MTSA requires that the Coast Guard carry out assessments of overseas ports to ensure they are compliant with the code. However, the agency has only a total of 13 International Port Security Liaison Officers (IPSLO) to cover all of Europe, the Middle East, Africa, Latin America and the Caribbean. There are only another half a dozen liaison officers available to do this for Asia. Presumably these inspectors should know something about port security, be familiar with commercial port operations, and understand the local circumstances, but there is no formal training program in place to develop all these skills. A single country like Brazil may have over 25 ports, but a typical country assessment visit will involve a 2-3 day country trip and include a visit to just one port.

A Coast Guard inspector visiting an overseas port will likely find that he is following a well worn path. A foreign port could have hosted a Naval Criminal Investigative Service (NCIS) visit. Its terminals may have been subjected to a security audit by U.S. companies under the Customs Trade Partnership Against Terrorism Program. There

could be a team of U.S. customs inspectors operating in the port as a part of the Container Security Initiative. The port may have hosted a visit by the State Department's Export Control, and Related Border Security Assistance (EXBS) program and the Energy's Department's Second Line of Defense & Megaports programs. It is unlikely that any of these visits will have involved interagency coordination in advance.

Under the Container Security Initiative protocol, customs agents will be working with their counterparts to target "high-risk" containers. That determination will be made by examining cargo manifests which must be submitted electronically to CBP 24 hours before it is loaded aboard a ship destined for the United States. But the cargo manifest is notoriously error prone and general and will not even include information such as where the container originally loaded.

In short, the flurry of U.S. government initiatives since 9/11 may create the impression that substantial progress is being made in securing the global trade and transportation system. Unfortunately, all this activity should not be confused with real capability. For one thing, the approach has been a piecemeal one, with each agency pursuing its signature program or programs with little regard for the other initiatives. There are also vast disparities in the resources that the agencies have been allocated. Then there is the issue of very weak intelligence that underpins the agency's assessments of risk. Further, in an effort to secure funding and public support, agency heads and the White House have oversold the contributions these new initiatives are making towards addressing a very complicated and high-stake challenge. Against a backdrop of inflated and unrealistic expectations, the public will be highly skeptical of official assurances in the aftermath of a terrorist attack involving the intermodal transportation system.

We can do better. With relatively modest investments and a bit of ingenuity, the international intermodal system can have credible security while simultaneously improving their efficiency and reliability. What is required are a series of measures that collectively enhance visibility and accountability within global supply chains.

As a starting point, the United States should work with the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in authorizing third parties to conduct validation audits of the security protocols contained in the International Ship and Port Facility Security Code and the World Customs Organization's new framework for security and trade facilitation. The companies carrying out these inspections should be required to post a bond as a guarantor against substandard performance and be provided with appropriate liability protections should good-faith efforts prove insufficient to prevent a security breech. A multilateral auditing organization made up of experienced inspectors and modeled on the International Atomic Energy Commission should be created to periodically audit the third party auditors. This organization also should be charged with investigating major incidents and when appropriate, recommend changes to established security protocols.

To minimize the risk that containers will be targeted by terrorist organizations between the factory and a loading port, Washington should embrace and actively promote the

widespread adoption of a novel container security project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong. Starting in late 2004, every container arriving at two of the truck gates in two of the busiest marine terminals in the world are, at average speeds of 15 kph, passing through a gamma ray machine to scan its contents, a radiation portal to record the levels of radioactivity found within the container, and optical character recognition cameras which photograph the number painted on the top, back, and two sides of the container. These scanned images, radiation profiles, and digital photos are then being stored in a database for customs authorities to immediately access if and when they want.

One of the benefits of the Hong Kong approach to container inspection is that it can help identify shielded objects that a radiation portal might not pick up and help to resolve a false alarm for benign shipments that have naturally occurring radiation level. A dirty bomb wrapped in lead may not set off the alarm of a radiation detector, but a gamma image would identify it as a dense object with a suspicious shape in a shipment of sneakers. Alternatively, a radiation portal might register an alarm when examining benign objects like ceramic tiles but by capturing a scanned image at the same time it will be possible to identify the shape of the materials is consistent with what is advertised on the cargo manifest. In this case, the container would not require an additional inspection, thereby reducing the amount of cargo that is pulled from the terminals under the CSI protocol. This in turn would reduce the risk that a container will miss its voyage because of the difficulty in getting it back from the inspection facility in time to be reentered into the outbound vessel's loading plan.

The way that CBP could best make use of the non-intrusive inspection data collected by the system being piloted in Hong Kong is tie the amount of images that they examine to the alert level set under the ISPS protocol. Under Level 1 or the normal alert level, customs inspectors would examine the data as a primary screen only for the high-risk containers they have targeted for inspection using their current algorithm, plus a random sampling of other containers. Under Level 2, they would double or triple the number of containers they look at by using their same risk-based formulation, but by expanding the pool of inspected containers by lowering the targeting floor by several notches and conducting more random inspections. This will essentially require their surging more inspectors to examine these extra images during the period of heightened alert. In the worst case, under Level 3—which would likely be set after a major terrorist incident—CBP would have to surge enough people to examine every container. This might seem overwhelming at first glance, but even if they took no advantage of software-assisted inspection tools and did the 5-minute manual manipulation of a image that field inspectors currently do, with 26,000 containers arriving in U.S. ports each day, this would require 2170 man-hours per day, or roughly 300 inspectors to examine—not an impossible task for the presumably limited window of time the country would be operating under at Level 3.

In addition to a sustained and systematic effort to bolster the security of the global intermodal transportation system by advancing the use of NII equipment in overseas

ports, the White House and Congress must simultaneously invest in securing America's neglected waterfront. There are seven things that must be done right away.

First, over the next 18 months, the Department of Defense must work closely with the U.S. Coast Guard, now part of the Department of Homeland Security, and with local authorities in organizing and participating in exercises that involve simulated attacks on the nation's largest commercial seaports. The training should focus on identifying what is required to quickly restore the operations of the port in the aftermath of a successful attack. These exercises and planning efforts must be a joint DoD-DHS effort, but should also include international maritime industry observers who will be affected by a major U.S. port closure and will need to take the lead on making the appropriate near-term adjustments to reduce the risk of a system failure.

Second, DoD needs to take the lead on funding and setting up joint operations centers in all major U.S. commercial ports: to outfit them with advanced information and communications technology that support surveillance and data sharing, and to provide the necessary training to the local, state, and federal agency participants. The resources and skill sets to accomplish this is concentrated within the national security community. It would be too costly and time consuming to try and develop these capabilities without the support of the military. This should be completed by 2007.

Third, the U.S. Navy should reposition one of its two salvage ships in Norfolk, Virginia to the West Coast and take the lead in drawing up commercial salvage contracts to support domestic harbor clearance. Over the next five years, the Navy should double its salvage fleet from four vessels to eight, and base two of them on the West Coast, two on the Gulf Coast, and two on the East Coast. The remaining two can be deployed overseas to support navy operations.

Fourth, the National Oceanographic and Atmospheric Administration (NOAA) hydrographic research vessels should receiving additional funding to complete bottom surveys of the all the major U.S. commercial seaports. This baseline information is indispensable in quickly spotting mines should an adversary deploy them. Without it, the centuries of junk that lay on the floors of most harbors have to be examined by divers to determine if they pose a risk. This post-mining examination could take many weeks or even months in the absence of current bottom survey data.

Fifth, the Coast Guard needs to see a doubling to $2.0 billion of the annual funding to replace its ancient fleet of vessels and aircraft, and to bring it command and control capabilities into the 21st century. Many of its cutters, helicopters, and planes are operating long beyond their anticipated service life and are routinely experiencing major casualties. Under the current delivery schedule, it will be 20-25 years before it has the kind of assets it needs today to perform its mission. This could leave a two-decade gap in capability as the existing fleet becomes too decrepit and dangerous to operate.

Sixth, Congress should authorize the reallocation of all the duties and fees that are collected in seaports to go back into the ports to support security upgrades and infrastructure improvements. Currently, ports are the only transportation sector where the federal

government is parasitic. That is, unlike airports and highways, the federal treasury takes more money away than its returns. According to the Coast Guard, seaports need to invest upwards of $5 billion to put in place minimal access control and physical security measures. Neither the ports nor their city of state governments have those kinds of resources.

Finally, the Customs and Border Protection Agency should receive $20 million in additional funding to expand the information technology capabilities and staffing at its national targeting center so that it can manage the NII scanning data collected in overseas terminals.

Against this backdrop, it should come as no surprise that my assessment of the national security implications of the DP World purchase of Peninsular and Orient Navigations systems and the leases to five containers terminals on the East Coast and New Orleans is that this commercial transaction will not *qualitatively* effect the overall state of global and American maritime transportation security. Stated differently, should a U.S. company assume control of these terminal operations tomorrow, it would not qualitatively improve our security. This is because the problem is less about who owns and operates U.S. container terminals than it is that we simply have not addressed far more serious supply chain, maritime, and port security issues that would dramatically reduce the terrorist risk to our homeland.

In the end, as our dependency on global trade grows and the catastrophic terrorist threat persists, the White House and Congress must start acting as though our commercial seaports are the critical national security assets they are. There should be fewer more urgent priorities than making sure America's ports and the transportation system responsible for moving the overwhelming major of world trade possess adequate capacity, redundancy, and resiliency to meet the daunting challenges that lie ahead.

Thank you and I look forward to responding to your questions.

Stephen Flynn is the author of *America the Vulnerable*. He is currently writing a new book to be published by Random House in Fall 2006 entitled, *The Edge of Disaster: Catastrophic Storms, Terror, and American Recklessness*. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report "*America: Still Unprepared—Still in Danger*," co-chaired by former Senators Gary Hart and Warren Rudman. Since 9/11 he has provided congressional testimony on homeland security matters on fifteen occasions. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issues on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.

For the Record

Eddie Bernice Johnson

The Honorable Eddie Bernice Johnson
Opening Statement
House Subcommittee on Coast Guard and Maritime Transportation re: Port Security
Thursday, March 9, 2006 – 2167 Rayburn

Thank you Mr. Chairman.

First let me extend my appreciation to you and Ranking Member Filner for your leadership on this issue and also allowing Members of the Full Committee to come and share our views.

Without question, today's hearing on the security of U.S. Ports is vitally important and extremely timely.

Less than two weeks ago, the Aviation Subcommittee held a hearing on the Bush Administration's proposal to ease laws governing foreign ownership and control of U.S. airlines.

Now, in what appears to be a trend—the Administration is now backing a deal to allow the United Arab Emirates to take over 6 major U.S. Seaports.

I suppose the next vital transportation asset to be turned over to foreign interest will be our interstATE highway system.

The Administration's handling of this situation exhibits a clear and blatant disrespect for the legislative branch of this government.

I strongly oppose foreign control of our U.S. seaports and domestic airlines and have added my name to the growing list of bipartisan opposition to these short-sighted proposals.

It is clear that, behind closed doors, the Committee on Foreign Investment decided to act in the interest of commerce over the security of our country.

To think that commercial and managerial control over our ports and airlines by foreign interest will have no implication on the security and safety of the American people underscores the short sightedness of these inept proposals.

Any modification to laws governing AND PORTS foreign control of domestic carriers will have enormous implications for industry stakeholders, security, and jobs here at home.

As a result, such decisions should not be hastily promulgated through rulemakings or decisions made behind closed doors and without input from the Congress.

The Congress should be afforded the opportunity to perform the necessary due diligence, conduct hearings, and debate any proposed changes to foreign ownership laws.

These ill advised and short sighted proposals should be stopped dead in their tracks.

I support the halting of this transaction and hope that we as a Congress continue to proactively exercise our oversight obligation on this matter.

Thank you and I yield back.

03/09/2006 16:15 FAX 202 226 2524 CG&MT SUBCOMMITTE 002

3-9-06 Hrg. For the Record

Statement of Congressman Mark Kennedy for the Coast Guard and Maritime Transportation Subcommittee hearing on Thursday, March 9, 2006

Mr. Chairman, I'd like to thank you for holding this hearing today on Dubai Ports World's (DPW) pending acquisition of P&O Shipping Company.

As we all are aware, this transaction, recently approved by the Committee on Foreign Investment in the United States (CFIUS), would transfer control of commercial operations of several major ports ~~in New York, New Jersey, Baltimore, New Orleans, Miami, and Philadelphia,~~ from a British corporation to a Dubai-owned corporation.

Although after its initial 30-day review, CFIUS found that this transaction would pose no threat to our national security, Members on both sides of the aisle have since ~~expressed concern about letting a foreign government-owned company manage these vital ports.~~ questioned this conclusion.

I share their concerns—Congress's ultimate and paramount responsibility is the security of the American people. While it is clear that Dubai has been an ally in the War on Terror and was one of the first Middle Eastern countries to join the U.S. Container Security Initiative, serious questions ~~remain about whether it is in our national security interest to turn operational control of our critical infrastructure over to an entity owned by any foreign government, however friendly it may seem.~~ have been raised about the level of its cooperation in other security matters. Congress has a duty to conduct oversight on matters that affect our national security and in today's post-9/11 world, matters of port security demand rigorous review.

That's why I, and several other Members, called for this oversight hearing related to the P&O-DPW transaction. While any foreign corporation which operates U.S. ports is bound by federal port security laws and regulations, we cannot leave any credible concerns uninvestigated.

Mr. Chairman, I am pleased that the Subcommittee will today hear testimony on this fundamental question, so that we can act in the best way possible to ensure that our port security is not jeopardized.

~~Make no mistake—the issue at hand is whether we can guarantee that a transaction involving the foreign government operation of our ports will not be detrimental to our national security. It is a critical question and one that I hope we will get a better answer to today.~~

REVISED

Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

AMERICAN ASSOCIATION OF PORT AUTHORITIES
1010 Duke Street • Alexandria, VA 22314
Phone: (703) 684-5700 • Fax: (703) 684-6321

Testimony of Kurt Nagle

President & CEO
American Association of Port Authorities

Before the
House Transportation and Infrastructure Committee

Subcommittee on Coast Guard and Maritime Transportation

MARCH 9, 2006

Good morning. I am Kurt Nagle, President and CEO of the American Association of Port Authorities (AAPA). I thank you for inviting us to testify before your Committee on the implementation of the Maritime Transportation Security Act (MTSA) and areas where additional efforts are needed to meet the objectives of this law. AAPA is an alliance of the leading public ports in the Western Hemisphere and our testimony today reflects the views of our U.S. members.

Enhancing maritime security and protecting America's seaports from acts of terrorism and other federal crimes is a top priority for AAPA and U.S. port authorities. Much has been done since 9/11, but more is needed. Protecting America's ports is critical to our nation's economic growth and vitality, and is an integral part of homeland defense. Ports handle 99% of our overseas cargo by volume, enable the deployment of our military, and serve as departure points for millions of cruise passengers each year.

Protecting our international seaport borders is a responsibility shared by the federal, state, and local governments, public port authorities and private industry. The Department of Homeland Security takes the lead in protecting America's ports. This includes programs of the U.S. Coast Guard, Customs and Border Protection, Immigration, and Transportation Security Administration. Port authorities, for their part, focus on protecting the facilities where this international cargo enters and exits the country, including partnering with their tenants. The security blueprint for these facilities is the Maritime Transportation Security Act, which your Committee established, and which AAPA worked closely with you to enact.

Let me begin with some comments on the proposed DP World acquisition of P&O Ports. In reviewing a transaction of this type, it is the appropriate role of the federal government to determine if there are national security concerns with any proposed business arrangement involving non-US interests, whether that involves port operations or any other business. There should be is a rigorous process to appropriately consider and resolve those questions.

AAPA believes that the current 45-day process underway regarding the Dubai Ports World's acquisition of P & O Ports should be allowed to run its course prior to Congress taking any action either on this proposed arrangement, or on any blanket prohibition against a foreign government affiliated company from providing terminal operating services at U.S. ports.

With regard to individual business arrangements, public port authorities often have leases with terminal operating companies to operate port-owned facilities. Those leases typically provide that any assignment of a lease to a successor company, in the event of a merger or acquisition, must be approved by the port authority. Leases generally cannot be transferred or assigned without permission.

The recent focus on port security has made many question what else this country needs to do to secure our ports. My testimony today will focus on three areas where AAPA believes this country needs to make progress related to port security: 1) The Port Security Grant Program, 2)

The Transportation Worker Identification Credential (TWIC), and 3) Adequate resources for federal agencies responsible for port security.

THE PORT SECURITY GRANT PROGRAM

Soon after September 11, Congress established the Port Security Grant program to provide much-needed help to port facilities to harden security to protect these vital ports of entry from acts of terrorism. The program has been authorized in several bills – the MTSA and Coast Guard reauthorization bill of 2004 – but it is only in the next round of grants (FY'06) that the program will mirror the authorization bills.

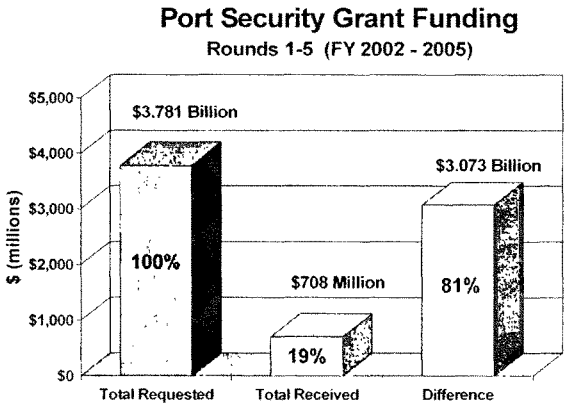
While there are a number of federal cargo security programs, this is the only program only that is focused on providing federal financial assistance for port facility security.

While the program has provided much-needed funding, it still had several problems:

1) An inadequate amount of funding;
2) Limits on eligibility;
3) The Administration's proposals to lump port security into a larger Transportation Infrastructure Protection (TIP Program); and
4) Slow release of the funding by the Department of Homeland Security (DHS).

Let me begin with the funding level. From its inception, the PSG program has been dramatically under-funded. While billions of homeland security dollars have been allocated to airports, first responders, and research and development, only a modest amount has been made available for port facility security improvements. For FY'06, DHS has stated that it is proposing $3.1 billion for port security, but last year's funding level for the Port Security Grant program was only $175 million. To date, DHS has given out $700 million in port security grants, but this is less than 20% of the grant requests, which totaled $3.8 billion (see chart below). AAPA recommends an annual funding level of $400 million for this program.

Since September 11, ports have spent millions of dollars of their own funds on port security. Ports have spent money on personnel and operations and maintenance of these expensive security systems, in addition to paying for security upgrades that the federal program did not pay for. However, more needs to be done. We have a good start and baseline, but we must continue our progress. Trade is growing exponentially and many port facilities are planning port expansion projects in response. Limited port security funds have placed large burdens on ports as security programs compete with funds required for general maintenance of facilities, channel dredging and port expansion projects. The biggest impact of funding limitations, however, is a delay in making security enhancements. Limited funds, mean slower progress.



This low level of annual funding has resulted in DHS limiting the eligibility of the program. AAPA is strongly opposed to this policy. Last year DHS decided to limit eligibility to 66 seaports based in part on the volume of cargo they handle. Half of our Association's membership was no longer eligible to apply. While we support a risk-based system, we believe that each port facility that must meet the requirements of the MTSA should be able to apply and make its case for assistance. We also are concerned that limits on eligibility might leave a class of perceived under protected ports. The MTSA states that the grants should be issued in a fair and equitable way. AAPA believes strongly that all facilities that are subject to the MTSA should be eligible for the grants, as was the case for the first four rounds.

The Administration also sought to eliminate the Port Security Grant program during the last two years by lumping port security into a Targeted Infrastructure Protection Program. Ports would have to compete for limited funds with domestic security grants such as intercity rail and bus security. This proposal was rejected by Congress last year, and we hope that Congress will continue its opposition. This is not the time to dilute the focus on port security. It should remain as a separate, dedicated program.

One final point on the grants: AAPA is concerned by DHS' slow pace in making the funds available. This delays the ability of ports to install security enhancements. For example, for FY'06, DHS opened the State Homeland Security grants in early December 2005, but we are still waiting for the Port Security Grants – nearly six months after the Appropriations bill became law.

IMPLEMENTATION OF THE TWIC

The second priority for AAPA related to port security is quicker implementation of the Transportation Worker Identification Credential – the TWIC. The MTSA included a provision that DHS develop a program that requires all individuals who have unescorted access to a secure area of a port facility or vessel undergo a background check to ensure they do not pose a terrorist security risk. While TSA has undertaken several pilot projects, four years after this law was

enacted, we are still far from implementing a TWIC system nationwide. AAPA and its members are frustrated by the delays in beginning the regulatory process.

TSA must make some policy decision regarding who should get the card, what the background check encompasses, and what is entailed in the appeals process. These are all policy issues that are separate from the technology challenges that the program faces. Uncertainty regarding compatibility with the pending TWIC has also caused delays in port implementation of access control systems.

ADEQUATE RESOURCES FOR FEDERAL AGENCIES

The final area AAPA believes should be a priority for port security is ensuring that adequate resources are available for the federal agencies with primary responsibility for port security. The U.S. Coast Guard and Customs and Border Protection are the two key agencies that need necessary resources to address port security. Both have done a great job to address these new challenges. Congress, however, needs to carefully evaluate whether the resources provided are adequate to do the job.

The U.S. Coast Guard, for example, is responsible for waterside security and needs more resources to focus on this area. With 361 seaports in the U.S., is Coast Guard able to adequately provide waterside security for all these facilities?

CBP also is involved in several programs to provide layered security for cargo flowing through ports. There are many challenges. Several GAO reports note that limits on staff size impact the effectiveness of the Container Security Initiatives and other cargo security programs. Projections on container and passenger volumes show a huge increase at seaports in the coming years. Congress must take a closer look at whether DHS has the inspection manpower to handle this growth and ensure our safety without negatively impacting efficiency.

CONCLUSION

In conclusion, our nation has made great progress in enhancing port security since September 11, and we need to continue this progress. Three areas Congress can focus on are increasing funding for the Port Security Grant program, quicker implementation of TWIC, and providing adequate resources for federal agencies responsible for port security.

On behalf of the American Association of Port Authorities, I thank you for this opportunity to discuss port security and welcome any questions from the Committee.

STATEMENT OF
THE HONORABLE JAMES L. OBERSTAR
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
FOREIGN OPERATION OF U.S. PORT FACILITIES
MARCH 9, 2006

- Mr. Chairman, for the past four years, this Committee has been trying to get Congress and the Administration to focus on maritime transportation and port security.

- It has taken the Dubai Ports World takeover of Peninsular & Oriental Steam Navigation Company and its operations at five U.S. ports to finally get anyone's attention.

- Now that we have people's attention, I am hopeful that the Administration and Congress will address the enormous security failures which plague the entire chain of transportation of goods entering United States ports.

CFIUS Review Process

- The security failures begin with the process for consideration of the Dubai Ports World takeover of P&O. The 12 member agencies of the Committee on Foreign Investment in the United States (CIFIUS) unanimously agreed that no 45-day investigation of the Dubai Ports World takeover was required because the takeover could not affect the national security of the United States.

- Now, at the request of Dubai Ports World, the Administration is conducting a 45-day "investigation". Yet, nothing would suggest that this investigation is real.

- The President and the 12 Members of CIFIUS have taken the position that there are no security problems. A few days after learning of the approval of the takeover one month after it was approved by his Administration, the President threatened to veto any effort to overturn it. He stated: "[t]his deal wouldn't go forward if we were concerned about the security for the United States of America."

- Since announcement of the additional 45-day investigation, the President has continued to defend the Dubai takeover. To decide after the 45-day

investigation that there are security problems with the takeover would be embarrassing to the President and his Administration.

- CIFIUS cannot conduct a meaningful review – nothing would suggest that the Committee's recommendation is going to suggest that the President is wrong.

- In fact, Secretary of Homeland Security Michael Chertoff has already gotten the message. He has suggested that we are more secure if the deal goes through.

- This process and its assessment of our national security is an absolute failure.

MTSA Guiding Principle

- Regrettably, the CFIUS process is only one of many of the Administration's security failures. Three and one-half years since Congress enacted the Maritime Transportation Security Act of 2002 (MTSA) (pronounced "MITSA"), there is little to show for our efforts to secure the supply chain.

- The guiding principle of MTSA is that we must "push the borders out". If a container enters the United States with a weapon of mass destruction (WMD) inside with a GPS detonator – it is too late.

- Cargo containers must be scanned and inspected overseas.

- Containers must be inspected as they are stuffed and made secure with "smart seals" that allow government inspectors to detect tampering with the container.

MTSA Mandates not Implemented

- ***Port Security Grants.*** In 2003, the Coast Guard estimated that it will cost U.S. ports $5.4 billion for facility improvements over the next decade to comply with the Coast Guard's port security regulations. The American Association of Port Authorities believes that Congress should appropriate at least $400 million each year for port security grants.
  Action: To date, Congress has appropriated $883 million for port security grants, 16 percent of the necessary $5.4 billion. The Administration has allocated only $708 million of the available funds.

- ***Background Checks.*** MTSA requires DHS to prescribe standards for background checks for any individual that would have access to a secure area of a marine facility. *Section 70105.*

  Airport and airline workers are subject to background checks and more than 1.6 million fingerprint-based background checks have been completed.

  Truckers who haul hazardous materials are subject to fingerprint-based background checks and, over the next five years, as many as 2.7 million truckers (including Canadian and Mexican truckers entering the U.S.) will get such checks.

  Action: No background checks are required to enter the secure area of port facilities and the Administration has not prescribed standards for background checks.

- ***Foreign-flagged Vessel Security Plans.*** MTSA requires all foreign-flag vessels entering the United States to submit their security plan to the Coast Guard for review and approval. *Section 70103.*
  Action: The Coast Guard has not reviewed and approved foreign-flagged vessel security plans. The Administration interpreted the law to only require that the Coast Guard accept the certification by the foreign-flag state that the vessel has an adequate security plan.

  At my request, H.R. 2443, the Coast Guard and Maritime Transportation Act of 2004, as passed by the House, included a provision to clarify that all foreign-flagged vessels had to submit their security plans to the Coast Guard for review and approval.

  On May 6, 2004, Mr. Filner offered a Motion to Instruct conferees on the bill to insist on the House provision. The Motion was adopted by a vote of 395-19.

  Yet, the Administration, working with the Senate, opposed efforts to clarify the statute to ensure that the Coast Guard reviewed and approved foreign-flagged vessel security plans and no provision was included in the Coast Guard Authorization Act.

- ***Foreign Port Security Plans.*** MTSA requires the Coast Guard to conduct foreign port assessments to determine if the foreign port has adequate antiterrorism measures including cargo screening, access controls for authorized personnel, and security management. *Section 70108.*
  Action: The Administration has not completed these assessments for our largest trading partners or those countries that are most vulnerable to security breaches.

- ***Container Seals.*** MTSA requires that the Department of Homeland Security (DHS) prescribe standards and procedures for securing cargo and monitoring that security while in transit, including standards for tamper-resistant seals that will identify when a container has been breached. *Section 70116.*
  Action: The Administration has not prescribed standards for container seals.

- ***CT-PAT.*** These failures are compounded by the Customs-Trade Partnership Against Terrorism (CT-PAT) program, which allows shippers to self-certify that they adhere to security standards and then receive expedited clearance through U.S. ports with no necessary audit or verification that the shippers meet the requirements of the program.

- After three and one-half years of failure, it is time for Congress to act and mandate specific timetables for each of these unmet maritime security mandates.

- It is time to require that all containers are scanned at foreign ports before they enter the United States.

- It is time to mandate the necessary security regime to protect our communities from a terrorist using the marine transportation system as a stealth missile.

March 8, 2006

STATEMENT OF ROBERT SCAVONE,

EXECUTIVE VICE PRESIDENT,

P&O PORTS NORTH AMERICA, INC.

BEFORE THE HOUSE SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

Mr. Chairman and Members of the Committee,

My name is Rob Scavone. I am Executive Vice President of P&O Ports North America, Inc. Among my responsibilities is the supervision of our compliance with security requirements in the U.S. I am a member of the Board of Directors of the National Association of Waterfront Employers, or "NAWE" an association of marine terminal operators in the U.S., both American and foreign. I also serve as co-chairman of an advisory group to the International Standards Organization on matters of container security, which group includes all major international terminal operators.

The Subcommittee has asked for testimony concerning the ongoing implementation of several programs related to cargo security, and I thank you for the opportunity to submit my comments on those matters here today.

Transportation Worker Identification Credentialing

The most anticipated program from my perspective, among those that are pending, is the Transportation Worker Identification Credential, or "TWIC" program. We in the terminal operating side of the industry are well aware that this project has been slow in gestation, but we also recognize that the TWIC rulemaking is a substantial and complex undertaking. We are mindful of the fact that the procedures required in a final TWIC rule must work in conjunction with our terminal operating gate systems, and we have strived to work with the agencies to minimize problems with the TWIC when it is implemented. We further understand that challenges exist with respect to the technology for scanning the cards, and recording biometric data.

It is now our understanding that the target date for issuing a Notice of Proposed Rule Making for the TWIC program is now around July 1st. We are also aware that, in view of the delays that have occurred to the implementation of this program, some have proposed interim measures, such as immediate worker background checks, to be performed by the employers. We, as much as anyone, understand the sense of frustration with the extended timetable for this program. We ourselves have forestalled the installation of other identification-based access controls, in anticipation of this program. However, we strongly suggest that the insertion of the employer between the government and the

transport worker for the purpose of background checks will be counterproductive. The employers simply do not have the resources, capabilities, or access to information that the government has. More importantly, many of the workers who will require ID cards, such as truckers, are themselves owner-operators, with no employer other than themselves, and unrelated to the terminal operator. We urge this Subcommittee to encourage TSA to continue on the current path to finalize the TWIC program.

In terms of specific features, it must be recognized that the response time for a transaction with a TWIC card at our gates must be several seconds, at most. This argues against the use of a central national database. This may not be a significant problem, since most of the persons entering our gates, including truckers, would be local and repetitive, but it begs the question as to how much of the responsibility for hosting and supporting the data base should fall on the terminal operator. Clearly the terminal operator cannot be responsible to keep the data current, for example. And the terminal operator should not be responsible to host a substantial amount of such data on its own computer hardware in order to make the system work.

Security of the Global Supply Chain

Over recent times, we have become accustomed to hearing that our ports in the U.S. are the "most vulnerable" points of entry. This, in turn, tends to lead to the incorrect conclusion that the ports themselves are the *location* where security needs most to be enhanced. This is not correct. Our ports in the U.S. are *already* the one point in the supply chain over which we have the *most* control.

The main point is that, if the security of the supply chain *in a foreign location* should fail, the place where we in the U.S. will be first *exposed* to that failure would, of course, be in the U.S. port. However, no amount of security on the part of the terminal operator in that U.S. facility will change that.

Therefore, the enhancement of the security of our U.S. ports, and, by extension, our homeland, is best accomplished by improving the security at the point of origin. Of course, this concept is not new, and in fact such programs as the 24-hour rule, C-TPAT, and the CSI program, have all contributed to this goal. However, if efforts will be made to continually improve our security, this is where the focus must remain.

Such efforts will be focused upon such matters as: the integrity of container seals; improved capability to conduct non-intrusive inspections at the port of loading; upgrading of the Automated Targeting System; greater cooperation between U.S. Customs and the local customs officials; and related technologies to permit better tracking of cargo loads along the supply chain.

Some of these objectives will experience substantial progress via the simple decision to devote more resources to them. We in the industry urge this Subcommittee to do its part to see that this happens. Others will require a global, comprehensive government-

industry effort, which will include the governments of virtually every trading country, and both carriers and marine terminal operators, together with technology vendors, and international standards bodies such as ISO, the International Standards Organization.

Foreign Ownership

The fact that foreign interests own many of the companies that manage our terminals in the U.S. has recently become a major point of discussion. The focus has been on the extent to which such ownership may impact the security function inside our terminals. The answer is, it does not impact the security function at all, for the following reasons:

1. The Coast Guard and Customs continue to be responsible for all security measures relating to the entrance of persons or goods into the United States. Those agencies maintain a presence in the ports, and work with the Port and local police. Our terminals work in close cooperation with those authorities every day. The statement that the security of our ports is being outsourced is simply not the case.

2. Inside a terminal, only longshoremen perform any physical work on containers. By way of example, P&O Ports employs approximately 6000 longshoremen every day.

3. The terminal operator has no role in verifying or inspecting the declared contents of any container entering the United States. In fact, the terminal operator does not request from the carrier, nor does it require, any information concerning the contents, origin, or destination of the containers that it handles, unless, of course the cargo is declared to be hazardous, because those containers have separate handling procedures. That role is performed exclusively by U.S. Customs. No container leaves a U.S. facility until U.S. Customs indicates that it is free to go.

4. When Customs decides which containers will be opened, they do it with their own staff, not with the terminal operator's workers.

Mr. Chairman, thank you very much for the opportunity to provide these remarks today.

THE WALL STREET JOURNAL.

P&O Attracts Buyout Overture Amid Shipping-Industry Boom
By Jason Singer
31 October 2005
The Wall Street Journal

Peninsular & Oriental Steam Navigation Co. has received a buyout overture from a port operator in Dubai, according to a person familiar with the matter, in a potential deal that could be valued at nearly GBP 3 billion, or about $5 billion.

The United Arab Emirates company, Dubai Ports World, owned by the emirate of Dubai, sought a meeting for early this week with the British ports and ferries company, although the two sides haven't yet talked. There can be no assurances a deal will emerge, this person said. The offer was previously reported by London's Sunday Times.

P&O said in a statement yesterday it has been contacted by a third party but there have been no negotiations. A P&O spokesman declined to elaborate. A person at Dubai Ports World said nobody was available to comment.

If a deal emerges, it would be the latest in the rapidly consolidating industry of ports and container shipping, which remains the most popular mode of transportation for moving goods world-wide.

In May, A.P. Moeller-Maersk of Denmark, a large container-shipping firm, bought Royal P&O Nedlloyd NV of the Netherlands -- a smaller shipping company in which P&O held a 25% stake -- for 2.3 billion euros ($2.78 billion). Shipping firms are finding they need greater economies of scale as business amid a boom in the business fueled in large part by the transport of Chinese exports world-wide.

Earlier this month German tourism and transportation conglomerate TUI AG received the necessary backing from shareholders in CP Ships Ltd. to buy the U.K. shipping company for about 1.74 billion euros, making TUI the fifth-largest marine shipper by volume.

Port operators around the world have been consolidating. PD Ports PLC of the U.K. said earlier this month it had received a takeover approach from an unidentified suitor, and British ports operator Mersey Docks & Harbour Co. was purchased by rival Peel Ports in September for GBP 771 million.

P&O has been considered a potential takeover target since Maersk purchased Royal P&O Nedlloyd. That sale slimmed the U.K. company into a focused port operator with terminals world-wide. P&O has a market value of about GBP 2.3 billion.

Last week, the company reduced its 2005 profit expectations because lower consumer-spending in the U.K. had damped business at its two British terminals. Should Dubai Ports pursue a deal for P&O, it is expected several other global port operators in Hong Kong, Singapore and elsewhere may also consider a bid for P&O.

Founded in 1837, P&O is considered one of the world's top port operators after hiving off its container-shipping unit. The company has 27 container terminals around the world and also runs logistics services in more than 100 ports in 18 countries. In the U.K., P&O is also one of the top ferry operators.

Dubai Ports World has grown through acquisitions. It bought the international-terminals business of CSX Corp. for $1.15 billion in 2004, which launched it to the top leagues of global port operators.

***

The Journal of Commerce

P&O Ports in play
By Peter T. Leach
14 November 2005
Journal of Commerce

Whoever wins the nascent bidding war for the assets of Britain's venerable Peninsula and Oriental Steam Navigation Co., the outcome will clearly spell a victory for P&O management's efforts to unlock the value in those assets. The outcome also will underscore the high premium that investors place on the consistent earning power of container ports and terminals, in contrast to the much more cyclical earnings of ocean carriers.

"In the same way that CP Ships and P&O Nedlloyd attracted quite a premium because of their scarcity value as listed companies, I would assume that P&O Ports would attract quite a premium as well," said Mark Page, director of Drewry Shipping Consultants in London. "When you buy P&O, primarily it's the ports you're getting, because it doesn't come with too much additional baggage."

P&O Ports, the world's fourth-largest port operator, represents the value in P&O's assets, because it generates 80 percent of the group's profit. P&O operates 27 terminals and logistics centers in 100 ports in 18 countries, with 2004 throughput of 22 million TEUs.

P&O's ferries division is losing money and has been a drag on company earnings, and hence its share price. P&O's management has been considering ways of spinning off the ferries division, but Dubai Ports International, which made a surprise offer for the entire company at the beginning of November, apparently was unwilling to wait for that eventuality.

"What I always thought would happen was that everyone was waiting for the ferries to be sold, so that you would have a pure port company," Page said. "But what is happening is that because of the scarcity value of these listed companies, Dubai Ports said, 'We can't wait for the ferries to be sold, so we'd better get it now and we'll get rid of the ferries.' "

Dubai Ports, which became the world's fifth-largest port operator last year through its acquisition of CSX World Terminals, approached P&O's management in late October with an unsolicited offer. The bid could value the company at nearly $7 billion, compared with its market value of $4.1 billion before the offer. The bid, which was not clearly defined, was quickly leaked to the press, put P&O in play, and drove P&O's stock price up 40 percent.

In the wake of the news, an array of global port operators and carriers are said to have contacted their investment bankers and to be preparing counteroffers. Potential bidders whose names have been mentioned include Temasek Holdings, the investment arm of the Singapore government, which already owns PSA Ports, the world's second-largest container terminal operator; APM Terminals, the port-operating division of A.P. Moller-Maersk; and Hutchison Port Holdings, the port division of Hong Kong's Hutchison Whampoa and the world's largest port operator.

Mediterranean Shipping and CMA CGM are reported to be watching the fray closely in the hopes of picking up some of the ports and terminals that the winning bidder will inevitably have to sell off. "In any portfolio of ports, there are bound to be certain ports that don't necessarily make sense for the acquiring company either because the regulators frown on them or because it may already have a terminal in that harbor," Page said.

European regulators would certainly frown on the potential antitrust issues that would be raised by a successful counteroffer by Hutchison Port Holdings. Concerns over competitive issues could force Hutchison to sell some of the British and North European ports that it might acquire.

In the U.K., P&O Ports has stakes in terminals in the ports of Tilbury and Southampton and has received approval to build a new port and logistics center at London Gateway in Thurrock, Essex. Hutchison's interests in the U.K. include terminals it owns and operates in the ports of Thamesport, Harwich and Felixstowe.

P&O's port interests in Europe include facilities in Antwerp and Le Havre on the Atlantic and Marseilles-Fos on the Mediterranean. Hutchison operates and/or owns terminals in Rotterdam, Willebroeck (near Antwerp), Gdynia in Poland, and at Germany's inland port of Duisburg.

There apparently would be no antitrust problems in the United States, but U.S. politicians might make noise over Hutchison's acquisition of P&O Ports, which operates in the Port of New York and New Jersey, Philadelphia, Baltimore, Miami, New Orleans and Houston. A few conservative members of Congress have complained that the Hong Kong-based company's operation of ports at Balboa and Cristobal at either end of the Panama Canal gives China control of the strategic waterway.

Whatever the outcome, P&O's shareholders stand to benefit from its management's efforts of the last few years to clean up the company's portfolio of holdings. The effort began in 1994, when it sold P&O Cruises to Carnival Cruise Lines. In 1996 it spun off its container division into a joint venture with Royal Nedlloyd, which became P&O Nedlloyd, in which it retained a 25 percent stake until it was sold to A.P. Moller-Maersk this year. P&O subsequently divested or sold off real estate holdings in ports around the world. Most recently, it sold off P&O Cold Logistics, the third-largest cold

storage and distribution operator in the world, to Versacold Holding of Canada for 183 million pounds ($320 million).

Whether P&O's management had ever intended to prepare the company for sale as a result of these beautification efforts, that is the almost inevitable outcome now. "It has resulted in realization of shareholder value," Page said. "Before this, no one would have been interested in taking it over."

***

FT FINANCIAL TIMES
World business newspaper

Dubai's DP World seals Pounds 3.2bn purchase of P&O.
By Robert Wright
29 November 2005
Financial Times

Dubai's DP World is to buy P&O, the UK container ports and ferries group, for Pounds 3.19bn.

After the deal - to be announced today - DP World, the container terminal operator owned by Dubai's ports and freezones authority, will be nearly as big as the world's third biggest container terminal operator, Denmark's APM Terminals.

The price offered for P&O - which announced pre-tax profits before exceptional items of Pounds 170m on Pounds 3.06bn sales for 2004 - could make a counterbid from a rival large container port operator unlikely, analysts said.

The bid is thought likely to come at about 440p a share - just above last night's closing share price of 435p.

P&O announced it had received an approach - without revealing from whom - on October 31, after a newspaper story linked the company to DP World.

DP World's concerns about P&O's pension liabilities and projections on the cost and likely revenues of P&O's planned London Gateway port development have been resolved.

The deal will bring to an end the independent existence of a company that was founded in 1837 - the year Queen Victoria came to the throne - and was once one of the key institutions of the British empire, taking civil servants, soldiers and mail between the UK and India.

Robert Woods, chief executive, is set to make more than Pounds 2.7m from selling his shares andexercising his share options after the deal. Lord Sterling, former chairman, will make about Pounds 10m.

The pair were instrumental in restructuring P&O, turning it from an unfocused conglomerate with a range of shipping businesses into the present operation, which has only container ports, ferries and a few residual property interests.

Neil Davidson, container ports analyst for London-based Drewry Shipping Consultants, said it was hard to see anyone else coming up with a bid to defeat DP World's. Mr Davidson said there would now be four heavyweight worldwide container terminal operators - Hong Kong's Hutchison Ports, Singapore's PSA, APM, part of the Maersk Group and DP World.

DP World became the world's sixth largest container terminal operator this year when it bought CSX World Terminals, the terminals business formerly owned by the US Railroad.

P&O had long been seen as a bid target because of its excellent assets across the globe, but particularly in China and India.

***

February 28, 2006

PRESS STATEMENT

With regard to questions raised during the US Senate Committee on Commerce, DP World Senior Vice President Michael Moore said,

"DP World does not discriminate and has not been charged with violating any anti-boycott statutes. DP World, as a global port management company, facilitates trade with many nations. Our company has long-standing business relationships with Israeli companies among our diverse international clients."

For further information please contact:

Office: +1-202-756-5046/7
Mobile: +1-202-361-7320

***

February 26, 2006

PRESS STATEMENT

DP World has today given a voluntary, formal commitment to separate P&O's U.S. operations held through P&O's wholly owned U.S. subsidiary P&O Ports North America, Inc. (POPNA).

In addition, with a view to addressing concerns regarding the original review by the Committee on Foreign Investment in the United States (CFIUS), DP World has today formally requested to be subject to a further CFIUS review.

Terms of the Hold Separate Commitment

As announced last Thursday, DP World intends to complete the $6.85 billion global transaction as scheduled, but will voluntarily separate out the U.S. assets that would otherwise be part of the deal to permit the Bush Administration, Congressional leadership and relevant port authorities to seek additional information regarding the acquisition.

The formal commitment, which is in addition to commitments made by DP World to CFIUS last month, states that:

- DP World will guarantee the independence of all terminal operations managed by POPNA by establishing the operations as a completely separate business unit.

- DP World will not exercise control over or influence the management of the U.S. operations -- either directly or via P&O headquarters in London.

- Final authority over the management and operations of the U.S. terminals rests exclusively with the Chief Executive Officer of P&O in London who is a British citizen.

- The Chief Security Officer for POPNA will remain a U.S. citizen, unless the U.S. Coast Guard agrees otherwise.

- The current management of POPNA will be retained and DP World will not in any way influence or attempt to influence any operations, policies, procedures, or security in place in the U.S. operations.

The above arrangement will remain in place until the earlier of May 1, 2006 or the completion of the additional CFIUS review which DP World and POPNA have requested.

Request for CFIUS Review

DP World and POPNA today issued a formal request to CFIUS that the committee initiate an immediate further review, including the full 45-day investigation authorized under U.S. law, of the acquisition of POPNA by DP World.

Ted Bilkey, Chief Operating Officer, DP World, said:

"We recognize that there are concerns regarding DP World's acquisition of P&O's U.S. terminal operations. Despite having already obtained approval by the federal government, we continue to take voluntary steps to assure people that the security of the U.S. will not be harmed as a result of this acquisition."

"We are confident the further review by CFIUS will confirm that DP World's acquisition of P&O's U.S. operations does not pose any threat to America's safety and security. We hope that voluntarily agreeing to further scrutiny demonstrates our commitment to our long-standing relationship with the United States."

For further information please contact:

Office: +1-202-756-5046/7
Mobile: +1-202-361-7320

***

February 23, 2006

PRESS STATEMENT

The acquisition by DP World of The Peninsular & Oriental Steam Navigation Company ("P&O") is a global deal covering 30 terminals in eighteen countries, ferries, and property interests at an acquisition cost of $6.85 billion. The U.S. assets represent less than 10% of this portfolio. It is not only unreasonable but also impractical to suggest that the closing of this entire global transaction should be delayed.

However, we appreciate that there are many people in the U.S. who have expressed concerns about DP World taking over the operations of P&O in the U.S., even though we have given formal commitments to the government of the United States that the management and structure presently in place at those ports will stay the same. We went through the legal approval process mandated by Congress that we were required to go through. Additionally, we passed every security standard in a review conducted by twelve separate departments and agencies of the U.S. government. Finally, we obtained all of the clearances required of other countries involved.

In light of this situation, DP World advises that:

1. DP World intends that the acquisition of P&O will proceed as planned. P&O's shareholders voted overwhelmingly for the transaction. DP World intends that the closing and payment to P&O shareholders will take place on schedule.

2. DP World will segregate P&O's U.S. operations while it engages in further consultations with the Bush Administration and as appropriate Congressional leadership and relevant port authorities to address concerns over future security arrangements at P&O's U.S. ports, which are today in full compliance with all U.S. security requirements. In practice, this will mean that DP World will not exercise control over, or otherwise influence the management of, P&O's U.S. operations pending the outcome of these further discussions.

Ted Bilkey, Chief Operating Officer for DP World, said the following:

"DP World has been working for many years with U.S. Customs, Navy and other U.S. security officials at its ports in Dubai to ensure the protection of the United States. We are highly respected for the efficiency and integrity of our operations. The reaction in the United States has occurred in no other country in the world. We need to understand the concerns of the people in the U.S. who are worried about this transaction and make sure that they are addressed to the benefit of all parties. Security is everybody's business."

For further information please contact:

Office: +1-202-756-5046/7
Mobile: +1-202-361-7320

HOLD SEPARATE COMMITMENT AND

REQUEST FOR CFIUS REVIEW

DP World FZE has made an offer to acquire all of the outstanding shares of The Peninsular & Oriental Steam Navigation Company ("P&O"), and the shareholders of P&O have voted overwhelmingly to accept DP World's offer. In order to allow the global transaction to proceed as planned while delaying taking control of P&O's U.S. operations held through its wholly owned U.S. subsidiary P&O Ports North America, Inc. ("POPNA") and to permit more time for consultation between DP World and the Bush Administration, Congressional leadership and representatives of various port authorities, DP World announced on February 23, 2006 that it would not exercise control over or otherwise influence the management of P&O's U.S. operations for an interim period. The purpose of this document is to memorialize and expand upon that announcement.

Further, DP World and POPNA jointly filed a notification to CFIUS on December 15, 2005. CFIUS completed a thirty (30) day review of that notification with a statement of no-objection dated January 17, 2006 (the "Original Notification") which induced DP World to declare the CFIUS condition of its offer to be met and so allowing it to proceed with the acquisition of the global operations of P&O without the need for further U.S. approvals. Such acquisition will therefore proceed as planned. However, with a view to addressing new concerns that have been raised, DP World and POPNA are hereby requesting to be subject to a further CFIUS review subject to the terms set out below.

I. Definitions

As used in this document:

A. "DP World" means DP World FZE acting on behalf of its parent companies, subsidiaries and affiliates (including Ports, Customs and Free Zone Corporation and Thunder FZE).

B. "P&O" means The Peninsular & Oriental Steam Navigation Company, a company created by Royal Charter in the United Kingdom and listed on the London Stock Exchange.

C. "POPNA" means P&O Ports North America, Inc., a wholly-owned subsidiary of P&O.

D. "Hold Separate U.S. Port Operations" means all of P&O's U.S. port operations managed by POPNA at various port facilities in the United States of America.

E. "CFIUS" means the Committee on Foreign Investment in the United States.

HOLD SEPARATE COMMITMENT

A. DP World hereby preserves and maintains the Hold Separate all U.S. Port Operations as an independent business unit, entirely separate, distinct and apart from all its other operations.

B. DP World will not exercise control over or otherwise influence the management of the Hold Separate U.S. Port Operations.

C. Final authority over the management and operations of the Hold Separate U.S. Port Operations are hereby specifically vested in and will be exercised by the Chief Executive Officer of P&O, who is located in London, England and who is a British citizen. DP World in Dubai will not exercise any such authority and will not in any way seek to influence such Chief Executive Officer's authority over the Hold Separate U.S. Port Operations.

D. DP World will retain the current management of POPNA ("POPNA Operational Management") to continue to manage and operate the Hold Separate U.S. Port Operations. DP World shall not transfer or terminate, or alter, to the detriment of any employee, any employment or salary agreement for, any current POPNA employee or for any union collective bargaining agreements.

E. POPNA Operational Management, and not DP World, have all rights, power and authority necessary to conduct the business of the Hold Separate U.S. Port Operations.

F. DP World will not influence or attempt to influence, directly or indirectly, POPNA Operational Management to alter any operational, security or any other policy or procedure now in effect at the Hold Separate U.S. Port Operations.

G. DP World will refrain from exercising any right to approve or appoint any director or officer of POPNA or any of its subsidiaries.

H. POPNA Operational Management have the sole and exclusive discretion to hire or fire personnel employed in connection with the Hold Separate U.S. Port Operations, consistent with current practices and labor agreements, security procedures and prevailing law.

I. The Chief Security Officer for POPNA will at all times be a U.S. citizen, unless the U.S. Coast Guard agrees otherwise.

J. DP World's influence over the Hold Separate U.S. Port Operations is limited to that necessary to carry out DP World's obligations under this Hold Separate Commitment and under any commitments previously offered to and accepted by CFIUS.

K. For the avoidance of doubt, notwithstanding anything contained herein, including DP World's agreement not to exercise control over or otherwise influence the management of the Hold Separate U.S. Port Operations, DP World shall be

entitled to the full economic benefit of ownership of P&O, POPNA and the Hold Separate U.S. Port Operations.

This Hold Separate Commitment shall take effect from the date on which POPNA becomes a member of the DP World group of companies (anticipated to be on or about March 1, 2006) and shall remain in effect until the earlier of May 1, 2006 and the date on which any further CFIUS review as referred to below is concluded.

REQUEST TO BE SUBJECT TO FURTHER REVIEW BY CFIUS

DP World and POPNA hereby jointly respectfully request CFIUS, on a non-precedential basis, to conduct a CFIUS review, including a full forty-five (45) day investigation, of the acquisition of POPNA by DP World. Upon prompt agreement by CFIUS to conduct such a review, DP World and POPNA will submit a notification to CFIUS, with this Hold Separate Commitment as an exhibit thereto, to initiate the requested review. DP World and POPNA will abide by the outcome of the review, but nothing herein shall constitute a waiver of any rights of DP World or POPNA that have arisen from the Original Notification.

Dated: February 26, 2006

P&O Ports North America, Inc.

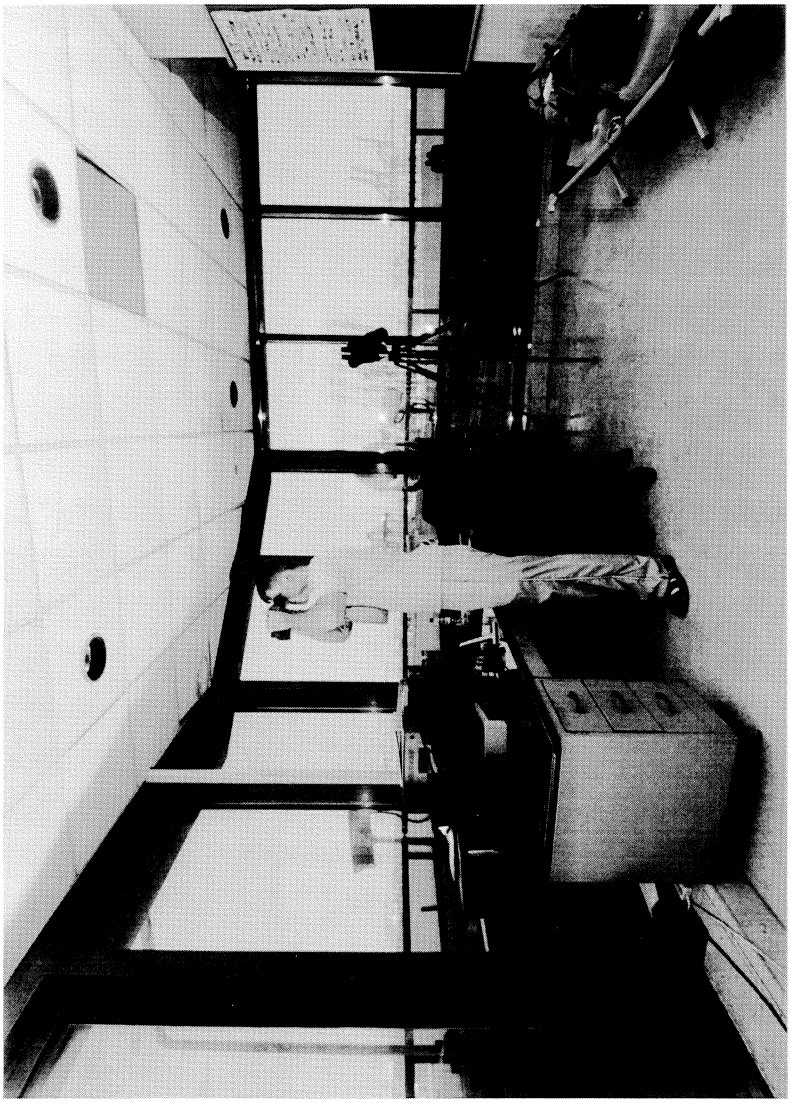
Michael Seymour

President

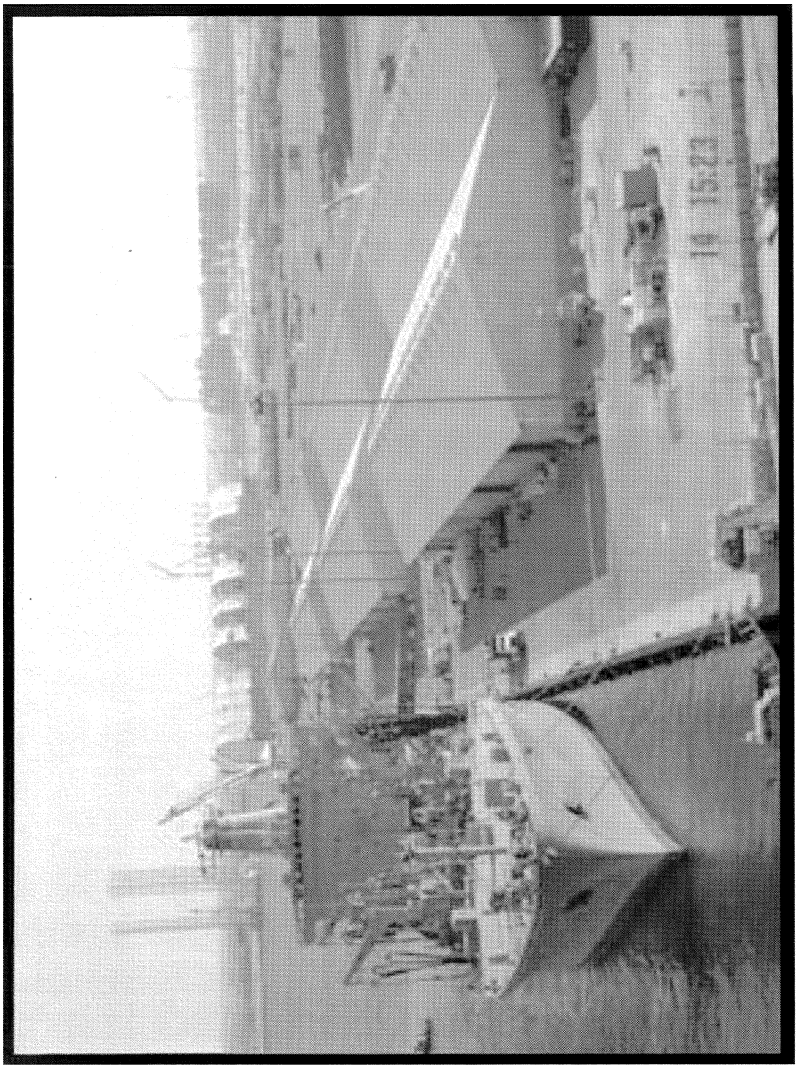
DP World FZE

H. Edward Bilkey

Chief Operating Officer



US Navy Officer in DP World Marine Control Tower Dubai



U.S. Navy Warship at its secure facility in DP World Dubai

Ms. Salma Hareb, CEO of Jabel Ali Free Zone (JAFZA), Mohammed Sharaf, CEO, DP World (slightly behind), HE Ismail Omar Guelleh, President of Djibouti, Sultan Amed bin Sulayem, Chairman

Sultan Ahmed bin Sulayem, Chairman of DP World and Vice Admiral Patrick Walsh on board the USS Vicksburg in Djibouti

Ports, Customs &
Free Zone Corporation

مؤسسة الموانئ
والجمارك والمنطقة الحرة

February 21, 2006

The Honorable Stewart Baker
Assistant Secretary for Policy, Planning & International Affairs
US Department of Homeland Security
Washington, DC 20528

Ms. Gay Hartwell Sills
Director, Office of International Investment
US Department of the Treasury
Washington, DC 20220

Dear Mr. Baker and Ms. Sills:

On behalf of the Ports, Customs & Free Zone Corporation and P&O Ports North America, Inc., we wish to advise that we have no objection to the Treasury Department and/or the Department of Homeland Security publicly releasing our letter of January 6, 2006 and the letter of January 13, 2006 from DHS in response.

Ports, Customs & Free Zone
Corporation

P&O Ports North America, Inc.

WDC01/231114v1

ص.ب ١٧٠٠٠، دبي، الامارات العربية المتحدة هاتف : ٨٨١٥٠٠٠-٤-٩٧١+، فاكس : ٨٨١٦٠٩٣-٤-٩٧١+
P.O. Box 17000, Dubai, United Arab Emirates Tel. : +971-4-8815000, Fax : +971-4-8816093
Website : http://www.jafza.ae, http://www.dpa.ae

U.S. Department of Homeland Security
Washington, DC 20528

**CONFIDENTIAL PURSUANT TO SECTIONS 552(b) (3) AND (4)
OF THE FREEDOM OF INFORMATION ACT,
5 USC SECTIONS 552(b) (3) AND (4), AND
SECTION 721(b) OF THE DEFENSE PRODUCTION ACT,
50 USC APP. SECTION 721(b)**

JAN 1 3 [redacted]

Thomas E. Crocker
Alston & Bird LLP
601 Pennsylvania Avenue NW
Washington, DC 20004

Robert Scholssberg
Freshfields Bruckhaus Deringer LLP
701 Pennsylvania Avenue, NW
Washington, DC 20004

Dear Sirs:

The purpose of this letter is to acknowledge the enclosed January 6, 2006, letter providing joint representations and commitments to the U.S. Department of Homeland Security (DHS) from your clients, the Ports, Customs and Free Zone Corporation, a Dubai public corporation established by Dubai Royal Decree under Law No. (1) of 2001 (PCFC), the Peninsular & Oriental Steam Navigation Company, a company incorporated by Royal Charter in the United Kingdom and listed on the London Stock Exchange (P&O), and P&O's wholly owned U.S. subsidiary, P&O Ports, North America Inc. (P&O North America), with respect to the proposed acquisition by PCFC of P&O through PCFC's wholly owned subsidiary, Thunder FZE, a Dubai corporation, which will also result in the acquisition by PCFC of P&O North America. We appreciate that you and your clients contacted DHS and others in the U.S. Government well in advance to provide a complete factual briefing. Next, the above-referenced acquisition was brought formally to the Committee on Foreign Investment in the United States (CFIUS) on December 15, 2005, in a joint voluntary Notice filed by Thunder FZE and P&O North America.

In consideration of these joint representations and commitments, memorializing our discussions and DHS requirements, DHS notified the Chair of CFUIS on January 6, 2006, that DHS had no objections to the above-referenced transaction. You will of course be notified of final CFIUS action by the CFIUS Chair.

Thank you for working cooperatively with DHS and others in the U.S. Government to responsibly address mutual concerns. DHS hereby acknowledges receipt of your clients' letter dated January 6, 2006, and agrees that the joint commitments stated therein become effective if and when the proposed acquisition by PCFC of P&O closes.

Sincerely,

Stewart A. Baker
Assistant Secretary for Policy,
Planning, and International Affairs

Enclosure

**CONFIDENTIAL PURSUANT TO SECTIONS 552(b)(3) AND (4)
OF THE FREEDOM OF INFORMATION ACT,
5 USC SECTIONS 552(b)(3) AND (4), AND
SECTION 721(b) OF THE DEFENSE PRODUCTION ACT,
50 USC APP. SECTION 721(b)**

January 6, 2006

Stewart A. Baker
Assistant Secretary for Policy, Planning, and International Affairs
United States Department of Homeland Security
Washington, DC 20528

Dear Mr. Baker:

This letter outlines the joint representations and commitments of Ports, Customs and Free Zone Corporation, a Dubai public corporation established by Dubai Royal Decree under Law No. (1) of 2001 ("PCFC"), Peninsular & Oriental Steam Navigation Company, a company incorporated by Royal Charter in the United Kingdom and listed on the London Stock Exchange ("P&O"), and P&O's wholly owned U.S. subsidiary, P&O Ports North America, Inc. ("P&O North America"), with respect to the proposed acquisition by PCFC of P&O through its wholly owned subsidiary Thunder FZE, a Dubai corporation, which will also result in the acquisition by PCFC of P&O North America. The commitments of PCFC, P&O and P&O North America contained herein shall only be effective if and when the proposed acquisition by PCFC of P&O closes.

This letter reflects the joint representations and commitments by these Companies ("the Companies") to the U.S. Department of Homeland Security (DHS) in connection with a joint voluntary Notice filed on December 15, 2005, with the Committee on Foreign Investment in the United States ("CFIUS") by the special purpose vehicle subsidiary of PCFC, Thunder FZE, and P&O North America, with respect to the foregoing described proposed acquisition. These joint representations and commitments are being provided for the purpose of providing assurances requested by DHS with regard to law enforcement, public safety and national security issues within the jurisdiction of DHS. These joint representations and commitments have been discussed with DHS and other CFIUS agencies in a series of briefings and follow up communications both before and after the aforementioned CFIUS Notice was filed for the purpose of providing supplemental information for those agencies to consider in exercising their role on CFIUS.

These Companies hereby confirm their joint representations and commitments to the following:

Maintenance of Membership, Cooperation, and Support in Security Arrangements

As was noted by the Companies in a briefing for CFIUS at the U.S. Treasury Department on December 6, 2005, the Companies represent and commit to maintain no less than their current level of membership in, cooperation with, and support for those Security Arrangements they currently participate in, as outlined in section 7(D) of the December 15 CFIUS Notice. Specifically, those Security Arrangements include the Customs-Trade Partnership Against Terrorism ("C-TPAT"), the Business Anti-Smuggling Coalition ("BASC"), and the Container Security Initiative ("CSI").[1] In addition, PCFC will continue to maintain their level of membership in, cooperation with, and support for the March 2005 Memorandum of Understanding with the U.S. Department of Energy to support CSI by cooperating and restricting the trafficking in nuclear and radioactive materials, in particular using the specialized equipment at Dubai's seaports terminals and training of personnel to inspect material and share information with respect to such material, as outlined in paragraph 5.6 of the November 17, 2005, "Project Thunder Background Briefing Paper for the [CFIUS]," ("Project Thunder Background Briefing") as amended December 15, 2005.[2]

The Companies further assure that, should they propose material changes with respect to maintenance of their level of membership in, cooperation with, or support for these Security Arrangements, the Companies will provide at least thirty (30) days advance written notice of such proposal to the Assistant Secretary of DHS for Policy, Planning, and International Affairs, detailing the reasons, timing, and plans for such proposed change. The companies further agree to meet and confer with any DHS designated U.S. Government officials prior to implementing such proposed change, to provide any relevant information requested with respect to such proposed change, and to reasonably address any security concerns raised with respect to such proposed change.

Management of U.S. Facilities

The Companies hereby represent and commit that their current intent and plan is to operate any U.S. facilities they own or control to the extent possible with the current U.S. management structure. These facilities include the U.S. persons being acquired as outlined in section 3 of the above-referenced CFIUS Notice.

Security Policies and Procedures, Officers, and Points of Contact for U.S. Facilities

The Companies represent and commit that they will maintain security policies and procedures at the U.S. facilities, under the direction of a responsible corporate officer, who will serve as a point of contact for DHS in any U.S. facilities owned or controlled by the Companies, including the

[1] The Companies will also continue to comply with all international and domestic Security Arrangements which are required by law and with which they have represented in the above-referenced CFIUS Notice they currently comply, such as the International Ship and Port Facility Security Code ("ISPS") and 33 CFR Subchapter H.

[2] PCFC will also maintain no less than the current level of membership, cooperation, and support for Security Arrangements pursuant to the terms of those Security Arrangements with the U.S. Armed Forces, including, in particular, the provision of services to U.S. Navy vessels and personnel at Jebel Ali Port, as noted in paragraph 5.7 of the Project Thunder Background Briefing, although these arrangements are outside the purview of DHS.

U.S. persons being employed as outlined in section 2 of the above-referenced CFIUS Notice. The companies further represent and commit that they will make any relevant information concerning these policies and procedures promptly available to DHS upon written request and will meet and confer with any U.S. Government official designated by DHS to address any concern.

Assistance to Law Enforcement

The Companies represent and commit that they will take all reasonable steps to assist and support federal, state and local law enforcement agencies, including but not limited to DHS agencies such as U.S. Customs and Border Protection, U.S. Coast Guard, and U.S. Immigration and Customs Enforcement ("ICE"), in conducting any lawful law enforcement activity related to any service provided in the U.S. by the Companies or their subsidiaries. Such assistance shall include, but not be limited to, disclosure, if necessary, of information relating to the design, maintenance or operation of the Companies' U.S. facilities, equipment or services. In particular, the Companies also agree to promptly provide, upon written request, any relevant records that may exist in the U.S., including matters relating to foreign operational direction, if any, of U.S. facilities owned or controlled by the Companies. The companies will maintain such records according to record retention policies adopted in the normal course of business of these facilities.

Non-Objection in CFIUS

The Companies understand that, promptly following execution of this letter by an authorized representative or attorney for the Companies and delivery thereof to DHS that DHS shall notify CFIUS that DHS has no objection to the proposed transaction described in the aforementioned CFIUS Notice.

The Companies further understand that, in the event that their joint representations and commitments as set forth in this letter are materially false or misleading, or the parties have omitted material information, DHS may (in addition to any other remedy available at law or equity) request that the CFIUS initiate a review of the Companies' application to determine whether such misstatements or omissions threaten to impair U.S. national security and, if it does, to determine an appropriate response to protect U.S. national security. In addition, in the event that these representations are otherwise materially nullified or breached, DHS may seek any other remedy available at law or equity.

Sincerely,

Ports, Customs and Free Zone Corporation

By: _____

P&O Ports North America, Inc.

By: _____
Robert Seymour, Executive VP

U.S. persons being acquired as outlined in section 3 of the above-referenced CFIUS Notice. The companies further represent and commit that they will make any relevant information concerning those policies and procedures promptly available to DHS upon written request and will meet and confer with any U.S. Government official designated by DHS to address any concern.

Assistance to Law Enforcement

The Companies represent and commit that they will take all reasonable steps to assist and support federal, state and local law enforcement agencies, including but not limited to DHS agencies such as U.S. Customs and Border Protection, U.S. Coast Guard, and U.S. Immigration and Customs Enforcement ("CBP, Coast Guard, and ICE"), in conducting any lawful law enforcement activity related to any service provided in the U.S. by the Companies or their subsidiaries. Such assistance shall include, but not be limited to, disclosure, if necessary, of information relating to the design, maintenance or operation of the Companies' U.S. facilities, equipment or services. In particular, the Companies also agree to promptly provide, upon written request, any relevant records that may exist in the U.S., involving matters relating to foreign operational direction, if any, of U.S. facilities owned or controlled by the Companies. The companies will maintain such records according to record retention policies adopted in the normal course of business of those facilities.

Non-Objection in CFIUS

The Companies understand that, promptly following execution of this letter by an authorized representative or attorney for the Companies and delivery thereof to DHS that DHS shall notify CFIUS that DHS has no objection to the proposed transaction described in the aforementioned CFIUS Notice.

The Companies further understand that, in the event that their joint representations and commitments as set forth in this letter are materially false or misleading, or the parties have omitted material information, DHS may (in addition to any other remedy available at law or equity) request that the CFIUS initiate a review of the Companies' activities to determine whether such misstatement or omission threatens to impair U.S. national security and, if it does, to determine an appropriate response to protect U.S. national security. In addition, in the event that these representations are otherwise materially nullified or breached, DHS may seek any other remedy available at law or equity.

Sincerely,

Ports, Customs and Free Zone Corporation

By: _____
Sultan Ahmed Bin Sulayem
Executive Chairman

P&O Ports North America, Inc.

By: _____

FACT SHEET: DP WORLD BACKGROUND

- DP World is a multinational company based on Dubai, which sits astride the shipping lanes from Europe and Africa to Asia.

- Jebel Ali in Dubai was the original cornerstone facility, the largest container port between Rotterdam and Singapore, and the tenth largest global terminal overall. DP World sprung from this base, which is growing to become a massive transhipment center and free zone that is expanding to 50 square miles, including a six runway airport.

- DP World is a commercial enterprise owned by the Dubai government. It is part of a group of highly successful commercial ventures that take advantage of commerce to fuel the economy. These include world-renown Emirates Airlines and landmark property developments both internationally and locally.

- DP World's global commercial ventures require an international diverse team. The renowned management team is truly multinational including citizens of the United States, Australia, United Kingdom, India and the Netherlands. For example the Chief Operating Officer, General Counsel and Head of Business Development are all United States citizens. This will be even more the case following the acquisition of P&O.

- DP World is a global ports and terminal operator that is internationally recognized for its quality, service and customer satisfaction. Since 2001 it has embarked on a growth strategy that will catapult it to top-three status. With the purchase of P&O it will have operations in 50 ports, 30 countries and six continents.

- DP World's recent transactions included the $1.14 billion purchase of US terminal and shipping concern CSX-WT in early 2005. The intended P&O takeover is part of a business strategy designed to make DP World a global heavyweight on par with Hong Kong's Hutchison, Singapore's PSA and Denmark's Maersk.

- DP World's purchase of P&O is largely funded through a $6.5 billion syndicated debt deal underwritten by Deutsche Bank and Barclay Bank which is currently being syndicated on the international banks market.

- DP World brings a unique suite of operational expertise: container terminals, general cargo terminals, free trade zones (including the world's largest), customs, and logistics centers.

***

FACT SHEET : THE ACQUISITION

- With the acquisition of P&O, DP World becomes the third largest global port terminal operator, with 51 terminals in 30 countries on five continents. Our capacity will be 50 million TEU.*

- This was a commercially driven and completely transparent takeover of a UK listed company underwritten by Barclays and Deutsche Bank. The purchase has been approved by P&O shareholders and the two companies are in the process of integrating.

- The ports industry is an economic cornerstone for Dubai. DP World believes that the offer for P&O has compelling strategic logic and creates significant opportunities for companies, customers and employees going forward. In particular, the combination:

  - Enhances DP World's position as a top 3 global ports operator
  - Addresses the needs of the customer base
  - Offers an unparalleled complementary geographical fit
  - Provides significant additional capacity in key markets
  - Brings together some of the most experienced people in the industry
  - Provides a strong company wiling to invest in much-needed infrastructure to support the growth of global trade
  - Provides complete continuity of management within P&O Ports North America Inc and further opportunities for growth in the Americas market.

- Currently, DP World operates 22 container terminals, 4 free zones and 3 logistics centers. DP World has operational offices in 15 countries. DP World's current capacity is 20 million TEUs. DP World also has a number of very large port development projects underway such as Pusan in South Korea, Qingdao in China and Cochin in India. The key numbers:

		DPWorld	P&O	Combination
Number of terminals	No.	22	29	51
Number of countries	No.	15	18	30
Current gross capacity	TEUm	20	30	50
Global ranking	No.	7	4	3

The terms: 520 p ($9.05) in cash for each outstanding P&O deferred share with a total value of 3.93 billion pounds Sterling ($6.85 billion) in cash.

** Twenty-foot equivalent unit, or half a standard size shipping container.*

***

FACT SHEET: SECURITY

- Globally DP World has received all the necessary regulatory approvals regarding the intended acquisition of P&O.

- In addition to the United States, P&O Ports operate in Argentina, Australia, Belgium, Canada, China, France, India, Indonesia, Mozambique, New Zealand, Pakistan, Papua New Guinea, Philippines, Russia, South Africa, Sri Lanka, Thailand and the United Kingdom.

- DP World existing operations are located in Australia, China, Dominican Republic, Germany, Hong Kong, India, Romania, South Korea, UAE and Venezuala.

- In the United States the purchase was approved by the Committee on Foreign Investment in the United States (CFIUS) on January 17, 2006. CFIUS implements an Exon-Florio provision to provide a mechanism to review and, if the President finds necessary, to restrict Foreign Direct Investment that threatens the national security. CFIUS includes 12 government departments and agencies:

  - Department of Defense
  - Department of Homeland Security
  - Customs and Border Protection
  - United States Coast Guard
  - Department of Transportation
  - Office of the United States Trade Representative
  - Office of Management and Budget
  - Office of Science and Technology Policy
  - Department of Treasury
  - Department of Justice
  - Department of Commerce
  - Department of State

  Unanimous approval was granted.

- Security at US ports is directly overseen by the United States Coast Guard and by Customs and Border Protection. P&O Ports North America Inc, is a long standing member of the Customs-Trade Partnership against Terrorism (C-TPAT). P&O Ports North America Inc is committed to maintaining and enhancing its leading role in C-TPAT.

- P&O Ports North America Inc, will continue to operate after the acquisition as the North American operating arm of the company. P&O Ports North America Inc will directly report to P&O SN Co in London. The management of P&O Ports North America Inc will remain in place unchanged.

- P&O Ports North America Inc, lease and operate terminals, they do not own ports. Through concession and operating agreements P&O Ports North America Inc provide services to Ports, Shipping Lines and Cargo Owners.

- Following two months of pre-application consultation with US Government Agencies, DP World and P&O Ports North America Inc jointly filed a notification of the acquisition

to the CFIUS on December 15, 2005, consistent with Section 721 of the Defense Production Act of 1950, as amended, and U.S Department of the Treasury Regulations at 31 CFR Part 800.

- The CFIUS reviewed the notification and concluded, by letter dated January 17, 2006, that the acquisition did not raise issues of U.S. national security sufficient to warrant an investigation.

- P&O Ports North America Inc and DP World have expressly committed to maintain and, as appropriate, expand all existing security arrangements and commitments of P&O Ports North America Inc. DP World already participates in US security programs in its global operations including the Customs Trade Partnership against Terrorism and the Container Security Initiative, which includes US Customs and Border Patrol offices in Dubai.

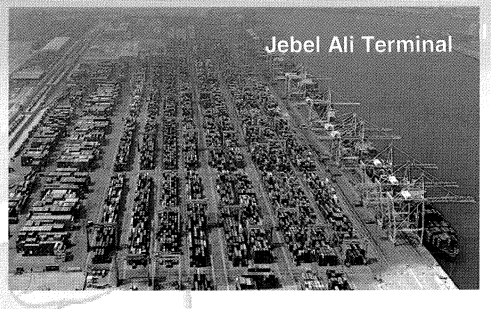
- The Governments of the United Kingdom and Australia reviewed in specific detail the P&O acquisition of operations in those countries by DP World and raised no objections to the transaction.

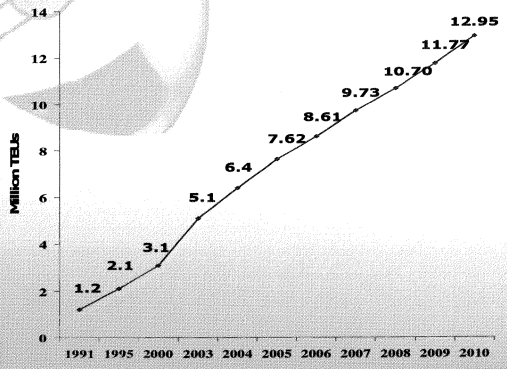
***

DP World Jebel Ali – A Flagship Facility

- Annual growth has averaged over 20% since 2002
- Handled 7.7M TEU* in 2005 (Jebel Ali & Port Rashid)
- The largest container port between Rotterdam and Singapore
- World's 9th largest container port

* 20-foot equivalent unit, or half a standard size container





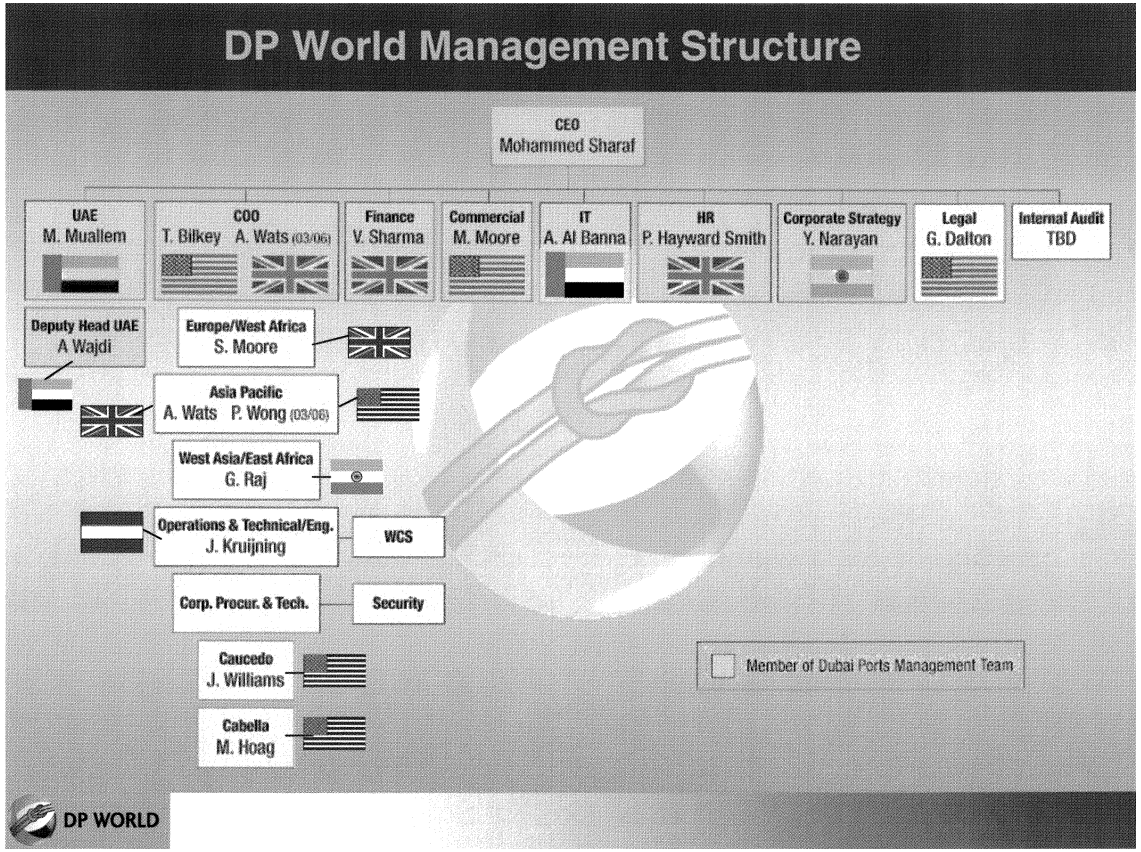
DP WORLD

Jebel Ali Free Zone: 242 American Companies

Jebel Ali Free Zone is a tax free enterprise zone that operated by DP World's sister company.

Regional headquarters and distribution operations for 242 American companies are located there, including several Fortune 100 companies.

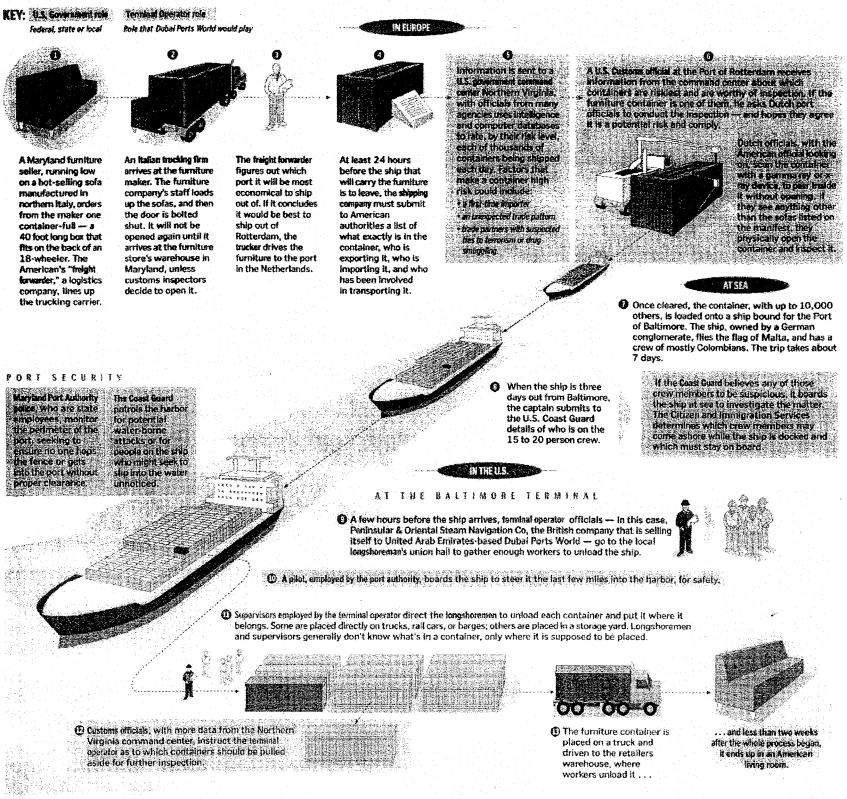
DP WORLD


DP World Management Structure
CEO
Mohammed Sharaf
UAE
M. Muallem
COO
T. Bilkey A. Wats (03/06)
Finance
V. Sharma
Commercial
M. Moore
IT
A. Al Banna
HR
P. Hayward Smith
Corporate Strategy
Y. Narayan
Legal
G. Dalton
Internal Audit
TBD
Deputy Head UAE
A Wajdi
Europe/West Africa
S. Moore
Asia Pacific
A. Wats P. Wong (03/06)
West Asia/East Africa
G. Raj
Operations & Technical/Eng.
J. Kruijning
WCS
Corp. Procur. & Tech.
Security
Caucedo
J. Williams
Cabella
M. Hoag
Member of Dubai Ports Management Team
DP WORLD

The Washington Post

How Cargo Travels Through the Shipping System
Reporting by Neil Irwin; Graphic by Laura Stanton
26 February 2006
The Washington Post

The Washington Post created this hypothetical example of how goods are brought into the U.S. via container ship based on interviews with shipping experts.



The Washington Post

U.S. Intelligence Agencies Backed Dubai Port Deal
By Walter Pincus
25 February 2006
The Washington Post

Reviews by U.S. intelligence agencies supported Dubai Ports World's purchase of the British company running terminals at six American seaports, and the assessments were made available to the Treasury Department-run interagency committee that approved the deal, according to senior administration officials.

The intelligence studies were coordinated by the Intelligence Community Acquisition Risk Center, a new organization under the office of the Director of National Intelligence John D. Negroponte, said one official. The center normally does broad threat analyses of foreign commercial entities that seek to do business with U.S. intelligence agencies.

Rep. Rush D. Holt (D-N.J.), a member of the House Permanent Select Committee on Intelligence, yesterday asked the panel's chairman, Rep. Peter Hoekstra (R-Mich.), to have a full briefing on intelligence reviews of the port deal and provide "any classified intelligence community assessments that are pertinent." Holt's concern is finding out how closely potential terrorism threats were examined, according to congressional sources.

While contents of the intelligence assessments remain classified, current and former intelligence officials yesterday spoke highly of the level of counterterrorism cooperation provided after Sept. 11, 2001, by Dubai and several of the other states that make up the United Arab Emirates.

A former senior CIA official recalled that, although money transfers from Dubai were used by the Sept. 11 hijackers, Dubai's security services "were one of the best in the UAE to work with" after the attacks. He said that once the agency moved against Pakistani nuclear scientist Abdul Qadeer Khan and his black-market sales of nuclear technology, "they helped facilitate the CIA's penetration of Khan's network."

Dubai also assisted in the capture of al-Qaeda terrorists. An al-Qaeda statement released in Arabic in spring 2002 refers to UAE officials as wanting to "appease the Americans' wishes" including detaining "a number of Mujahideen," according to captured documents made available last week by the Combating Terrorism Center at West Point. The al-Qaeda statement threatened the UAE, saying that "you are an easier target than them; your homeland is exposed to us."

One intelligence official pointed out that when the U.S. Navy no longer made regular use of Yemen after the USS Cole was attacked in 2000, it moved its port calls for supplies and repairs to Dubai.

Marine Corps Gen. Peter Pace, chairman of the Joint Chiefs of Staff, on Tuesday praised the "superb" military-to-military relationship with the UAE, saying, "In everything that we have asked and work with them on, they have proven to be very, very solid partners."

The new emir of Dubai, Sheik Mohammad bin Rashid al-Maktoum, who as crown prince was the UAE defense minister, also played a major role in pushing financial deals such as the Dubai Ports World's purchase of the firm, Peninsular and Oriental Steam Navigation Co. of London.

***

Associated Press

Foreign firms operating cargo port terminals are common in U.S. West Coast
By Alex Veiga
25 February 2006
Associated Press Newswires

An Arab company's potential takeover of some marine terminals at six major ports on the East Coast has raised questions about foreign operations at U.S. seaport facilities.

Yet, such arrangements have been commonplace at West Coast ports for years.

"On the West Coast, almost all the ports have their terminals operated by foreign companies," said Ivan Eland, senior fellow at The Independent Institute, a nonprofit, nonpartisan public policy research organization based in Oakland, California.

About half of the port terminals on the East Coast are managed by companies based overseas, he added.

Most of the cargo that enters the United States comes through huge ports in Los Angeles, Long Beach, Oakland and the Seattle-Tacoma area of Washington.

Each has marine terminals operated by foreign shipping lines -- many from Europe and Asia.

A political firestorm erupted this week after it was learned that the Bush administration approved a deal by United Arab Emirates-based Dubai Ports World to acquire London-based Peninsular and Oriental Steam Navigation Co.

Many lawmakers have voiced concern over whether the transaction could lead to possible security risks at docks where Dubai Ports would operate terminals.

Nearly all ports around the United States are owned by governments, which lease terminals to private companies that must adhere to security and labor rules as part of the deals, said Marc Hershman, a professor at the University of Washington School of Marine Affairs.

For decades, scores of firms ran cargo operations at U.S. ports. But many have been swallowed up by larger, foreign-owned companies.

"There has been a huge consolidation within the terminal operating world," Hershman said.

The bid by Dubai Ports to operate terminals at U.S. ports is not the first such move to spark opposition.

In the late 1990s, federal lawmakers cited national security concerns while killing a plan by China Ocean Shipping Co. to lease space at the former Long Beach Naval Station. The company now leases a terminal at the Port of Long Beach and operates it jointly with a U.S. firm.

Other foreign firms have encountered fewer roadblocks.

In 1997, Singapore-based Neptune Orient Lines acquired U.S.-based American President Lines, a major shipping company with operations along the West Coast, including Seattle-Tacoma.

"There was a lease (at the port) with them and the lease was just assumed by the new parent company," Hershman said. "The only moaning that went on is that we lost another U.S.-flagged carrier to foreign competition."

***

The New York Times

A Ship Already Sailed
By Simon Romero and Heather Timmons
24 February 2006
The New York Times

In the outcry over who should run America's seaport terminals, one clear trend appears to have been overlooked: American companies began withdrawing decades ago from the unglamorous business of stevedoring, ceding the now-booming industry to enterprises in Asia and the Middle East.

So it is no accident that American companies are not in the top ranks of global terminal operators, who have ridden the coattails of the explosion in world trade. That shift has transferred growing financial clout to a handful of seafaring centers in Hong Kong, Singapore and now the emirate of Dubai.

Indeed, the takeover of the Peninsular & Oriental Steam Navigation Company of Britain came down to a battle between two foreign, state-backed companies. One of them, DP World, is owned by Dubai's royal Maktoum family. The other, PSA, the world's second-largest port operator, is part of the Singapore government's investment arm.

The acquisition price also reflects the advantage that a number of the fastest-growing companies enjoy -- their governments' deep pockets. DP World paid about 20 percent more than analysts thought the company was worth. Publicly traded companies that were potential bidders were scared off long before DP World's final offer.

Some foreign operators also have been more profitable because they are vertically integrated: they operate terminals at the export site, manage the shipping lines that transport the cargo and then operate terminals that unload the cargo at the other end, often in the United States. Such soup-to-nuts management allows these operators to cut costs, increase efficiencies on high volumes and achieve higher margins.

Moreover, the international shipping business has evolved in recent years to include many more containers with consumer goods, in addition to old-fashioned bulk commodities, and that has helped lift profit margins to 30 percent, from the single digits. These smartly managed foreign operators now manage about 80 percent of port terminals in the United States. That figure is 90 percent in Britain, a country that used to be the world's biggest shipping power.

Though two American companies now rank eighth and ninth among the world's top 10 operators, it would not be easy for other American companies to get into the business. The retreat began decades ago amid rising labor costs and slow growth, while foreign companies spotted opportunities.

"For a long time in the United States, no one wanted stevedoring on their business card because it was not a glamorous job," said Prabir Bagchi, a specialist on supply-chain management at George Washington University. "Control of many of those low-paying jobs went east, and now look who's cheapest and best at providing customer service."

The biggest players in the global port and terminal management industry are a mixed group. Some are state-owned, some are publicly traded, some have shipping operations, and many are still run by wealthy families or their founders.

Hutchison Whampoa, the world's biggest container port operator, for example, is a conglomerate that is publicly traded in Hong Kong. The company's founder, Li Ka Shing, is often referred to as China's richest man, but the company has been priced out of recent bidding wars, in part because the Hutchison's mobile phone business is cash-strapped.

APM Terminals of Denmark is part of the shipping giant AP Moller Maersk Group, which is publicly traded but controlled by the Moller family of Denmark. The group has been buying up shipping assets, and purchased the container carrier P&O Nedlloyd in January.

"Certain port operations in certain locations recognized the potential years ago, and embarked on acquisitions," said Neil Davidson, a container ports analyst at Drewry Shipping Consultants in London. When approached, "P&O had an obligation to their shareholders," Mr. Davidson said. "An offer came in which was too attractive to turn down."

P&O earned $383 million on revenues of $2.4 billion in the first six months of 2005. The company itself grew in the United States through an earlier wave of industry consolidation, taking over local companies like Gulf Service of New Orleans in 2000 and International Terminal Operating Company of Jersey City in 1999. Similarly, Neptune Orient Lines of Singapore in 1997 acquired one of the oldest American terminal operating and shipping companies, American President Lines, which originated in the Gold Rush of 1848.

The opportunities for well-run foreign terminal operators to grow in the United States are clear. American ports are considered somewhat backward by shipping experts outside of the country.

For example, most major ports overseas operate 24 hours a day, seven days a week. But in the United States, ports were shut down at night until very recently. And transmitting shipping orders electronically to some American ports does not necessarily save time because the orders need to be rekeyed into the ports' computer systems, a concession to unions trying to preserve jobs.

Foreign terminal operators, on the other hand, have benefited by running several lower-cost port operations around the world in places such as Hong Kong, Singapore and Dubai, all of which have become huge export and transshipment centers for international trade. Ports in the United States operate largely as local ports, receiving ships with goods meant for nearby consumption.

"It's like we're used to flying out of a small airport while they've been using O'Hare or J.F.K.," said Bob Watters, vice president of SSA Marine, a family-owned company in Seattle that is the largest terminal operator in the United States and that has been a force behind developing a large transshipment port in Panama.

With large volumes of trade, some of these foreign operators have leveraged ties with their major customers, the large shipping lines, into much closer relationships. The arrangements resemble that of FedEx with Cisco Systems, where FedEx does everything from air and road transport to minor assembly to procurement from suppliers, said Mr. Bagchi, the professor at George Washington University.

People in the shipping industry have watched with dismay as their fast-evolving business is sometimes misinterpreted in the uproar over the $6.8 billion sale of a venerable British concern (W. Somerset Maugham wrote a short story about colonial intrigue titled "P&O") to a rising operator from Dubai. One example is the fact that DP World, P&O or their competitors would not actually run or manage the ports in the United States.

Instead, that function belongs to port authorities, the municipal-, county- or state-controlled entities that own and operate most American ports. Companies like P&O simply lease cargo terminals from the ports, akin to a landlord-tenant relationship.

At the Port of New Orleans, for example, P&O operates only 20 percent of the port's terminals, according to a spokesman, Chris Bonura, where it handles cargo like lumber and steel coming down the Mississippi River from the Midwest.

A terminal operator is now expected to manage where and when a ship will berth, the use of gantry cranes, relations with unionized stevedores and arrangements with trucks or rail cars to take goods to market. This is all done with specialized software intended to minimize the amount of time a ship stays in port, allowing owners to use the vessels as much as possible.

The rise of foreign terminal operators has shifted power in an increasingly vital industry. About 90 percent of the world's goods are transported by ship, and 90 percent of those goods travel in standardized shipping containers of the sort that arrive in container ports where DP World and others operate.

The standard-size containers and the concept of containerization was developed by a truck owner in New Jersey, who went on to found Sea-Land, a container company now owned by Maersk. The first container-laden ship left Newark's port in 1956.

Port authorities in recent years have come to rely much more on foreign terminal operators to help finance land acquisitions, dredging and other improvements, a development that has worried some advocates for American ports, particularly those ports that rely on some kind of public subsidy to survive.

In some cases foreign terminal operators have been able to use their size and importance to negotiate favorable leasing deals with port authorities that effectively prevent these ports from existing without public support in the form of taxes or other public money transfers, said Marc Hershman, a professor at the School of Marine Affairs at the University of Washington.

"These vertically operated companies have the cash to make things work in their favor," said Mr. Hershman. "Many local port authorities are ceding power in their partnerships with these companies, with oversight of labor, environmental and security issues being given over to their tenants."

Even with assurances from DP World and its supporters that it would hew to American security requirements, analysts, regulators and bankers have been scratching their heads at demands by politicians to review the deal, in part because the deal is already completed under British law.

"God knows how you'd reverse it," said one London-based executive involved in the sale, who did not want to be identified because of client confidentiality agreements. British regulators have approved the deal, and shareholders have already voted for it, he said.

"The Arabs own it, what are you going to do? Force them to sell it? Revoke their licenses for United States ports?" he asked.

Either of those measures might spark some sort of retaliation from Dubai in the form of legal action, he said, or even something as extreme as some sort of a restrictions on American-bound shipments passing through the port of Dubai.

***

The Washington Post

Port Problems Said To Dwarf New Fears
By Paul Blustein and Walter Pincus
24 February 2006
The Washington Post

For people who have grown anxious about U.S. port security because a Dubai company may soon manage operations at six container terminals on the East Coast, Kim Petersen suggests that the real grounds for concern lie elsewhere -- such as the fence he saw at a West African port a few months ago.

The newly built fence was a source of pride to the port's officials, who wanted to show that they were protecting their facility against any terrorists seeking to sneak a bomb aboard a U.S.-bound container. But it was a 51/2-foot-tall chain-link fence -- hardly sufficient for the task, said Petersen, president of SeaSecure, a maritime security firm in Fort Lauderdale, Fla.

The tale illustrates a point emphasized by many people familiar with security operations at U.S. ports: Among all the reasons to fret about vulnerabilities to terrorist attacks, the nationality of the companies managing the terminals is one of the least worrisome.

"There are many, many problems that we face in maritime security -- and they're not the United Arab Emirates," Petersen said, referring to the Persian Gulf nation of which Dubai is a part.

Nonetheless, politicians from both parties continue to pelt the Bush administration with criticism for its decision to allow Dubai Ports World, a fast-growing business owed by the Dubai government, to buy Peninsular and Oriental Steam Navigation Co., a British maritime firm that manages terminals in Baltimore, New Jersey, New Orleans and several other major ports. At a Senate Armed Services Committee hearing yesterday, lawmakers acknowledged that the UAE has become an important U.S. ally in the Persian Gulf region but repeatedly cited the UAE's role in recognizing the Taliban before the Sept. 11, 2001, terrorist attacks, and the lax supervision of its banking system that allowed some of the hijackers to finance their plans.

But such points bypass some crucial questions: What do the companies managing U.S. terminals -- most of which are owned by Asian and European shipping giants -- do that is so important to protecting against terrorist attacks? And how much difference would it make if Dubai Ports World joined their ranks?

Administration officials have asserted in recent days that security at U.S. ports is the responsibility of the Coast Guard and U.S. Customs and Border Protection, with the terminal operators responsible for little more than transferring containers from ships to railroad cars and trucks.

That overstates the role government agencies play. "They've been saying that customs and the Coast Guard are in charge of security; yes, they're in charge, but they're not usually present," said Carl Bentzel, a former congressional aide who helped write the 2002 act regulating port security.

The private terminal operators are almost always responsible for guarding the area around their facilities, although they must submit their security plans to the Coast Guard, which monitors and inspects them. In some cases, the companies X-ray incoming containers to see whether the contents appear to match the manifest, although customs agents are solely responsible for "intrusive" inspections -- that is, opening containers and examining the cargo. That procedure is performed on about 5 percent of containers entering the United States.

The security personnel employed by the terminal companies vary from port to port, but according to several companies, the guards are often supplied by local private security firms.

"The lowest-paying jobs on the waterfront are security people," said Stephen E. Flynn, a ports expert at the Council on Foreign Relations. "But is that a problem for foreign ownership? No. It's a problem for everybody."

Shifting ownership from Britain's P&O to Dubai Ports World would not affect those arrangements at the terminals in question, company officials said. Consider, for example, the situation at the Philadelphia port, where Dubai Ports World would obtain 50 percent control over a local outfit that runs one terminal out of eight leased from the Philadelphia Regional Port Authority.

Robert Palaima, who runs the local company, said yesterday that he hires guards from a union that provides security officers and police guards under a security plan approved by the Coast Guard, which carried out a full-day inspection this week.

Cargo loading and unloading is done by work crews supplied by the International Longshoremen's Association, which Palaima described as "the most patriotic of unions." And there would be no changes in the workforce even if the Dubai Ports World takeover goes through, he said, adding: "I am sick and tired of all this uproar. We're patriots and nothing will change."

Much more serious, in the view of Petersen and other experts, are gaps in security that have nothing to do with the Dubai takeover.

"We've spent barely $700 million in federal grants to U.S. ports for security, compared with almost $20 billion for aviation security," Petersen said. "And most important, we are doing an abysmal job in assisting ports in the developing world in improving security to even minimal acceptable standards."

Since 2001, Washington has arranged for customs officials to work in 42 foreign ports with rights to inspect containers before they head for U.S. shores; Dubai was the first in its region. But that covers only 80 percent of the containers entering the United States.

"If you're an al-Qaeda operative, you're going to send a bomb from a developing country where you know those safeguards don't exist," Petersen said. "That's the key flaw. We should be investing now in the countries that pose a real threat to our national security, with more security grants. But many of these ports don't even have adequate fencing or lighting."

***

The Washington Post

Uproar Surprised Dubai Firm
By Ben White
24 February 2006
The Washington Post

In the late 1990s, the government-owned company that would become Dubai Ports World was a relatively small domestic ports authority, managing ports in the United Arab Emirates city-state of Dubai.

Then it began buying terminals elsewhere in the Middle East, in India and in Europe.

In 2004, Dubai Ports World paid $1.15 billion for the global port assets of CSX Corp., which gave the company critical terminals in Asia and made it one of the 10 largest port terminal operators in the world.

Now its proposed $6.8 billion purchase of the 169-year-old Peninsular and Oriental Steam Navigation Co. of London (P&O), a vestige of the British Empire that operates ports in Baltimore, New York and other major U.S. cities, has touched off a huge political battle, vaulting the company outside the insular world of the global maritime industry. Dubai Ports World last night offered to delay part of the transaction, giving the White House more time to convince lawmakers that the deal does not present a security risk.

The rapid growth of Dubai Ports World mirrors the swift expansion of Dubai into a commercial power that is less and less dependent on oil wealth, which is modest by Persian Gulf standards. The glittering city-state has the Middle East's leading airline, Emirates, and has been snapping up other foreign assets, including the Essex House hotel in New York.

Dubai's leader, Mohammed bin Rashid al-Maktum, known as Sheik Mo, is the driving force behind the city's foreign investments and domestic building projects that include man-made islands shaped like palm trees, the world's tallest tower, an underwater hotel and a theme park to dwarf Disneyland.

Strategically located on the Persian Gulf, Dubai emerged in the late 1990s as a major port. So when the city began its ambitious economic growth campaign, becoming a global port operator made strategic sense. Now the company wants to expand into a new market, the United States, a massive importer of foreign-made goods.

Although the U.S. ports are causing the current ruckus, they are in fact only a small piece of P&O's business. But they are an important part of the deal because they would give Dubai Ports World a presence in a critical market where the company currently has no assets. "It's a strategic value. That's what's important," Chief Operating Officer Edward H. Bilkey said on CNN on Wednesday night.

Last night, in an offer coordinated with the White House, the company said it would not exercise control over U.S. port operations until further talks have been held between administration officials and lawmakers. The company said the rest of its transaction with P&O will move forward as planned.

"We need to understand the concerns of the people in the U.S. who are worried about this transaction and make sure that they are addressed to the benefit of all parties," Bilkey said in a statement. "Security is everybody's business."

The explosive fight over port security, direct investment in the United States by Arab countries and the secretive process by which the federal government reviews foreign purchases of potentially strategic domestic assets caught the company and others in the industry off guard. Dubai Ports World and P&O executives and maritime industry analysts had expected that the deal, first reported and discussed in October, would continue its smooth and anonymous path to completion on March 2.

"We did not expect this to happen. No one foresaw this in any way," said Michael Seymour, president of P&O's North American operations. "P&O and DP World thought we had gone through the regulatory process in considerable depth, both from an antitrust and a security perspective, and frankly, we thought we were there." One of the members of the review committee that approved the proposed purchase of the U.S. ports was Treasury Secretary John W. Snow, the former chairman of CSX. However, Snow left CSX in January 2003, almost two years before Dubai Ports World acquired the CSX port assets in December 2004.

Industry analysts said they anticipated the deal would spark some initial concern and merit a review by the Bush administration. But they said they thought it would go through with little trouble because Dubai Ports World is well-known and respected in the global port management industry, which is already dominated by non-U.S. companies and has no direct responsibility for port security.

"They have a sterling reputation," said Peter S. Shaerf, managing director of AMA Capital Partners LLC, a merchant banking firm that specializes in the maritime and transportation industries. "They have never done anything that would expose them in any way as a security risk. They run first-class ports."

Shaerf noted that while Dubai Ports World is owned by Dubai, many of its top executives, including Bilkey, come from the United States. Other top executives come from Britain, India and elsewhere. "All of them were at top companies" before joining Dubai Ports World, Shaerf said.

In an interview on CNN on Wednesday, Bilkey attempted to correct what he called a "complete misconception" by the public and politicians of what Dubai Ports World is and what it does.

"First of all, we're a commercial enterprise of the government of Dubai. The government of Dubai has nothing to do with us, basically," he said. "They're not involved in our daily operations. When we want to make investments, when we want to have a new project, we decide it on commercial terms. And we base it on financially sound operations. You know, DP World, even before this acquisition, was a very large operation, highly respected. And we have wonderful relations with global customers."

Operating port terminals requires a large initial investment but can quickly become profitable, analysts said. Operators make money by charging shipping companies to rent port equipment and by assessing handling and storage fees. Once they are purchased, port terminals are fairly inexpensive to run, so profit margins are high. Because it is very difficult and expensive to build new facilities, especially in Western nations that import heavily from Asia, companies in the terminal operation business grow mainly by acquisition.

Because it is owned by the Dubai government, Dubai Ports World does not disclose detailed financial information. On its Web site, the company says it has averaged better than 20 percent growth in the past three years. P&O discloses its financial information, and it is clear that Dubai Ports World is hoping to buy a profitable asset.

Not including a charge for restructuring its ferry business, P&O said it earned $327 million in 2004. Just $31.1 million of that came from ports in the Americas, indicating that the U.S. ports are only a small piece of Dubai Ports World's acquisition. P&O's Asian ports earned $162.4 million in 2004.

But analysts and other executives, who echoed Bilkey's comment on CNN, said the U.S. ports are critical because the shipping industry is consolidating, and big shippers want to deal with terminal operators that can handle shipments around the world. "All port operations are of a global nature," Seymour of P&O said. "The Americas may or may not be the most profitable at any given point in time, but you need to be in all the markets."

Dubai Ports World generally leaves its acquisitions untouched, keeping current management and workers in place. Seymour said operations at P&O's U.S. ports also would not change, something he said was made clear during the federal review process.

"DP World has given a clear understanding that they do not intend port management to change either at the corporate level or at any location. It is a black and white statement." He added that security at the ports would continue to be handled by local police, the Coast Guard and U.S. Customs. "The short answer is that absolutely nothing will change," he said.

In addition to other U.S. citizens, Dubai Ports World's leadership includes David Sanborn, President Bush's nominee to run the Transportation Department's Maritime Administration. Department of Transportation spokesman Brian Turmail said Sanborn, who is Dubai Ports World's head of European and Latin American operations, would not comment on the current fight, or any other matter, because the Senate has not voted on his nomination.

Turmail said Sanborn was selected for the maritime administrator's job because of expertise gained during 30 years in the industry. Turmail said Sanborn has been at Dubai Ports World less than 10 months and had no role in the company's negotiations to buy P&O. Turmail said Sanborn played a supporting role as the administration reviewed Dubai Ports World's proposed purchase of P&O. "As the process went through, he was asked questions about it," Turmail said.

***

The Washington Times

U.S. ceded control of ports
By William Glanz
26 February 2006
The Washington Times

The furor over a United Arab Emirates company taking over some operations at six U.S. ports underscores the global nature of the shipping industry and the minor role played by American interests.
Foreign-owned companies dominate the maritime industry amid the war on terrorism, and many U.S. ports would be drowsy backwaters without them.

The role of U.S. shippers, stevedores and terminal operators has declined since the late 1990s, when two shipping firms were bought by foreign competitors.

The Bush administration's quiet approval of Dubai Ports World's $6.8 billion purchase of Peninsular and Oriental Steam Navigation Co. (P&0), based in London, sparked a fierce public debate over port security and the threat of terrorists penetrating P&O operations.

The decision also shed light on the international nature of the shipping industry and underscores consumer ignorance of how everything from beer to automobiles is moved around the world.

"I'm willing to guess there's a very large segment of the U.S. population that doesn't know where many things are made, or more importantly, how they got from where they are made to the target in Peoria," says Michael Berzon, president of Mar-Log Inc., a Maryland supply-chain and supply-chain security consultant.

Scandinavian ships flying the flag of Panama, where the vessel is registered, employing Filipino workers, regularly sail into the Port of Baltimore. A German ship flying the Greek flag arrives weekly at the Virginia Port Authority's terminals in Norfolk with cargo from China.

"This is a global business, not an American business. Maybe we as an industry have not done a good job explaining that, but we've never been asked," says Peter S. Shaerf, managing director of merchant banking firm AMA Capital Partners LLC, in New York.

International operator

Mr. Shaerf describes Dubai Ports World as a respected, well-run terminal operator. Under the terms of purchase, the United Arab Emirates company would operate some terminals at six ports -- Baltimore, Philadelphia, Miami, New Orleans, New York and Newark, N.J.

In Baltimore, the company would take over operation of two of the 14 terminals. In addition to U.S. contracts, the P&O Ports acquisition covers ports in Vancouver, Canada, Buenos Aires and locations in Britain, France and several Asian countries.

Dubai Ports World, owned by the Dubai government, already operates 22 marine terminals in 15 countries, including China, India, Venezuela and Australia. Other ventures include trucking operations, freight transportation logistics, airport operations and business-enterprise zones.

The purchase was scheduled to take effect Thursday, but Dubai Ports World said late last week it will not exercise control over new operations in the U.S. while the Bush administration tries to soothe congressional critics and alarmed governors who raised concerns over port security.

President Bush said he will oppose efforts to block the transaction, and Dubai Ports World said it intends to complete its purchase of P&O.

The Treasury Department's 12-member foreign-investment committee reviewed the sale and unanimously agreed it posed no problem, according to the department.

Like others in the industry, Dubai Ports Chief Operating Officer Edward H. Bilkey last week said the company was puzzled by the U.S. response to the purchase.

"The reaction in the United States has occurred in no other country in the world," Mr. Bilkey said. "We need to understand the concerns of the people in the U.S. who are worried about this transaction and make sure that they are addressed to the benefit of all parties."

Global commerce

Dubai Ports World is surrounded by other foreign competitors at U.S. ports. Foreign businesses keep many ports running.

The top 10 containership fleets are based in Denmark, Switzerland, Taiwan, China, Germany, France, Japan, Hong Kong and Singapore.

The world's top terminal operators are not U.S. companies. Hutchison Port Holdings, the largest, is based in Hong Kong. PSA International Pse. Ltd., owned in part by the investment arm of the Singapore government, is the second-leading terminal operator. Dubai Ports World ranks seventh and would become the second-largest terminal operator, based on the number of containers handled, after its takeover of P&O.

"It's the reality of the globalization of commerce. Ports and terminal operations are no exception to that," says Kurt J. Nagle, president and chief executive of the American Association of Port Authorities, which represents 86 of the nation's public port authorities.

At the Virginia International Terminals, the operating arm of the Virginia Port Authority, Cooper/T. Smith Stevedoring and P&O Ports North America Inc., a subsidiary that would be owned by Dubai Ports World, announced they will combine operations in a new company to be called CP&O LLC. The merger is to be completed Oct. 1.

Stevedoring companies are hired by shipping lines to load and unload cargo ships. Ceres Marine Terminals Inc. is the Virginia port's other major stevedoring firm and is owned by Japanese shipping firm NYK Line. Norfolk also is the U.S. headquarters of CMA-CGM Group, a French shipping line, and Israeli shipper Zim-American Israeli Shipping Co.

Denmark's A.P. Moeller-Maersk, the largest terminal operator in the United States and owner of the world's largest shipping fleet, owns APM Terminals NA, which is building a $500 million private container terminal in Portsmouth, Va., scheduled to open next year. The terminal will be used solely by Maersk vessels.

"If you pulled the foreign shipping companies out of this port or any port, I don't know what we would do. It's as international a business as you can put your hands on," says Joe Harris, spokesman for the Virginia Port Authority, which operates three terminals.

America's role

There haven't been any major U.S. container shippers since Maersk bought Sea-Land Corp. from CSX Corp. in 1999. Maersk now navigates an operating fleet of 585 ships. That's more than twice as many vessels as its nearest competitor, Swiss-owned Mediterranean Shipping Co., with 282 ships.

While it was independent, Sea-Land had an operating fleet of 70 ships.

Neptune Orient Lines, in Singapore, bought California shipper American President Lines in 1997.

"America plays a very small role in terms of liner and container companies," Mr. Shaerf says.

The biggest American container shipper is Matson Navigation Co. Inc., in Oakland, and it ranks 31st in terms of shipping capacity with 18 ships, Mr. Shaerf says. Horizon Lines Inc., in Charlotte, N.C., with 16 ships, is the world's 35th-largest shipper.

Sea-Land is credited with starting the container shipping industry when it sailed a cargo ship from New York to Houston in 1956. The first trans-Atlantic container ships sailed 10 years later.

Landlords at ports

Among terminal operators, U.S. companies have a larger presence, but they are overshadowed by foreign competitors.

SSA Marine, a privately held family firm based in Seattle, is the world's ninth-largest terminal operator, based on the number of containers handled. It operates 105 terminals worldwide.

The four busiest U.S. ports are operated by government port authorities that act as mere landlords and contract with privately held firms such as SSA Marine and P&O to manage terminal operations.

The Port of Los Angeles, the nation's busiest port, has been run by private companies since 1911. It and the Port of Long Beach, Calif., account for 43 percent of U.S. imports.

Terminal operators want to expand their reach to manage terminals at ports in states including Georgia, South Carolina and Virginia, but those states are among 32 port authorities -- run by states, cities and counties -- that chose to operate ports on their own and shun the landlord approach.

South Carolina did employ terminal operators, but took back control of ports from unions to avoid labor strife. The port authority reported revenue of $130 million in fiscal 2005. The Virginia Port Authority reported fiscal 2005 revenue of $202 million.

"The industry wants to privatize," says Chuck Carroll, general counsel for the National Association of Waterfront Employers, a trade group representing private-sector terminal operators.

"It's not clear that privatization would help U.S. terminal operators compete with bigger, foreign-backed competitors.

Increasingly, the companies managing terminals are foreign businesses that also own shipping lines and unload cargo. In the fragmented shipping industry, behemoth foreign firms are in greater position to acquire smaller competitors and broaden their reach into more U.S. ports.

"Most people look at the port in Baltimore and say 'That's a port,' and they move on," Mr. Berzon says. "Now all of the sudden they say, 'Arabs are going to run the port.' Well, it's two terminals and it's an international business."

***

The New York Times

Big Problem, Deal or Not
By David E. Sanger
23 February 2006
The New York Times

WASHINGTON, Feb. 22 -- In the political collision between the White House and Congress over the $6.8 billion deal that would give a Dubai company management of six American ports, most experts seem to agree on only one major point: The gaping holes in security at American ports have little to do with the nationality of who is running them.

The deal would transfer the leases for ports in New York, Baltimore and Miami, among others, from a British-owned company to one controlled by the government of Dubai, part of the United Arab Emirates. But the security of the ports is still the responsibility of Coast Guard and Customs officials. Foreign management of American ports is nothing new, as the role already played by companies from China, Singapore, Japan, Taiwan and trading partners in Europe attests.

While critics of the deal have raised the specter that it might open the way to the "infiltration" of American ports by terrorists from the Middle East, the Dubai company would in most cases inherit a work force that is mainly American, with hiring subject to the same regulations as under the current British management.

Among the many problems at American ports, said Stephen E. Flynn, a retired Coast Guard commander who is an expert on port security at the Council on Foreign Relations, "who owns the management contract ranks near the very bottom."

It is clear that the questions involving the Dubai company, Dubai Ports World, have become a proxy for long simmering debates about security and a battleground for resurgent tensions between the White House and Congress. In the end, as Mr. Bush has discovered, the politics of globalization are local and emotional.

The unstated assumption behind the Democratic and Republican critique of the deal is that transferring corporate responsibility for the port terminal leases to a conservative Muslim country that bred two of the Sept. 11 hijackers increases the likelihood of another act of terror.

Some independent experts, like Dr. Irwin Redlener of the National Center for Disaster Preparedness at Columbia University, warn of the risk that "a lot of critical information about the movement of cargo is now accessible to new owners."

Mr. Bush, however, has suggested that the criticism of Arab ownership may have racial overtones. And in interviews Wednesday, officials of Peninsular & Oriental Ports North America, the British company that now manages the six terminals, dismissed the criticism as the imaginings of politicians who have little familiarity with American ports.

"We will still exist, with the same workers, and the same facility security plan, regulated by the same Coast Guard and Customs officials," Michael Seymour, who runs the operation, said in sketching what would happen if the Dubai company took over the management role. "And we'll be audited just as often -- maybe more often."

Such arguments are not likely to quell the debate, which is already turning to the question of whether the Bush administration cut some corners in speeding the review through the approval process to avoid the scrutiny that could touch off a political firestorm.

Among other battles playing out are whether the Bush administration is spending enough money on port security and whether it is focusing its energies on the right problems.

Another is whether the White House's case on port security is harmed by the fact that the major player is the Department of Homeland Security, whose failures after Hurricane Katrina will be the centerpiece on Thursday of a White House-directed report on "lessons learned" from the multiple failures in the devastation of New Orleans.

"The management of these ports is the door which you walk through to get to all of these other questions," said Senator John Kerry, Democrat of Massachusetts, who, like Mr. Bush, used cargo ports as the backdrop for speeches about the post-Sept. 11 world in 2004. "It raises a lot of questions about the lobbying, the connections and the terms of the deal, and the security problems the administration has left unaddressed."

It is also convenient for the Democrats, who are able to sound more hawkish on domestic security than President Bush. Mr. Bush finds himself burdened with the more nuanced argument that turning down this deal would send a message to the entire Arab world that it is not to be trusted, no matter how friendly individual countries may have been.

The administration's core problem at the ports, most experts agree, is how long it has taken for the federal government to set and enforce new security standards -- and to provide the technology to look inside millions of containers that flow through them.

Only 4 percent or 5 percent of those containers are inspected. There is virtually no standard for how containers are sealed, or for certifying the identities of thousands of drivers who enter and leave the ports to pick them up. If a nuclear weapon is put inside a container -- the real fear here -- "it will probably happen when some truck driver is paid off to take a long lunch, before he even gets near a terminal," said Mr. Flynn, the ports security expert.

That is where concerns about Dubai come in. While the company in question has not been a focus of investigations, Dubai has been a way station for contraband, some of it nuclear. Abdul Qadeer Khan, the Pakistani nuclear engineer, made Dubai his transshipment point for the equipment he sent to Libya and Iran because he could operate there without worrying about investigators.

"I'm not worried about who is running the New York port," a senior inspector for the International Atomic Energy Agency said, insisting he could not be named because the agency's work is considered confidential. "I'm worried about what arrives at the New York port."

That port, along with the five others Dubai Ports hopes to manage, are the last line of defense to stop a weapon from entering this country. But Mr. Seymour, head of the subsidiary now running the operations, says only one of the six ports whose fate is being debated so fiercely is equipped with a working radiation-detection system that every cargo container must pass through.

Closing that gaping hole is the federal government's responsibility, he noted, and is not affected by whether the United Arab Emirates or anyone else takes over the terminals.

***

FT FINANCIAL TIMES
World business newspaper

COMMENT & ANALYSIS: A steady pilot in the storm
By Robert Wright
25 February 2006
Financial Times

For anyone who has visited the Jebel Ali container port near Dubai City, which forms the heart of Dubai Ports World's operation, the wave of outrage in America in the the past two weeks over DP World's takeover of P&O has been particularly curious. In the minds of many US congressmen and women, the company from the United Arab Emirates seems to conjure up images of some mad Islamist intent on destroying the US and Israel. But one of the most striking impressions for a visitor to the port is likely to be the powerful bond between the operations at Jebel Ali and one man: Ted Bilkey, a 71-year-old American who is DP World's chief operating officer.

Tall, white-haired Mr Bilkey, who was born in Sun Valley, Idaho but grew up in New Jersey, became the sixth employee of the Dubai Ports, Customs and Free Zones Corporation when he was seconded to the newly-formed body in 1989 from SeaLand, then a major US container shipping line and now part of Denmark's AP Moeller-Maersk. He was among an influential group of westerners brought into Dubai around the same time by the ruling al-Maktoum family to build up the emirate's business interests and turn it into the Arabian peninsula's most important transport and financial hub.

Now as one of DP World's key executives, he is thought to retain a strong personal connection with Dubai's ruling family and a particularly strong bond with Sheikh Maktoum bin Rashid al-Maktoum, who decided to build the Jebel Ali port - the world's largest artificial port - and who died in January. Speaking of Mr Bilkey's relationship with Dubai, Michael Moore, DP World's senior vice-president (commercial) and another SeaÃ -Land hand, says: "He fell in love with the place." That bond, alongside the bluntly-spoken Mr Bilkey's wide-ranging knowledge of the US ports industry, made him the natural choice to front DP World's current drive to head off the opposition of US lawmakers and local port authorities to DP World's takeover of five US container terminals and other port-handling operations, including management of the New York City cruise terminal.

When DP World announced late in the week that it would press ahead with the P&O deal but segregate the US assets from the rest of the company, the quote on the statement was from Mr Bilkey - a rare step from a company whose public statements are nearly always made by either Mohammed Sharaf, the chief executive, or Sultan Ahmed Bin Sulayem, the chairman.

However, Mr Bilkey himself was perhaps the most powerful message. His first job on graduating from Yale University was clerical, on the docks in New Jersey. He served in the US Navy and was also at one time vice-president of New York's Maher Terminals, still the largest container terminal operator in the Port of New York/New Jersey. After a lifetime in the container ports industry, he is widely regarded as its elder statesman and is well liked despite a sometimes gruff exterior, according to industry insiders.

He has built up a like-minded, international team - including many Americans - around him. If this man and his team cannot be trusted to run US port terminals, the message seems to go, who can? "He's our most senior and experienced executive," Mr Moore says. "He's renowned in international trade He's thefellow with the real, hands-on experience of what goes on with security . . . "

Yet it is in Dubai that it is easiest to appreciate the vital role Mr Bilkey has played in steering Dubai's port operator from relative obscurity in the world container ports industry to the point where, when the deal goes through, DP World will be the world's second largest container terminal operator by throughput. The basis of the company's growth has been the port at Jebel Ali - the largest artificial port in the world. When Mr Bilkey arrived, it was handling 30,000 containers a year. He personally oversaw the drive which had made it, by 2004, the world's 10th-busiest container port, handling 6.42m 20-foot units (TEUs) of containers.

When showing visitors around, he points out the details that are vital to him and which have helped to make the terminal famously efficient. The engines in the gantry cranes which handle containers at the port were specially ordered to withstand sand from the surrounding desert. After the port became briefly congested during a surge in container trade in 2004, Mr Bilkey ordered some of the world's largest container cranes to ensure there would be no repetition - and there has not been.

On the P&O transaction, Mr Moore says that while the strategic direction came from Mr Sharaf and Sultan Sulayem, Mr Bilkey oversaw the handling of the deal's operational aspects. Yet the past two weeks have been tough, even for so indefatigable a character. "They're trying to keep me busy here," he told the FT on Friday. According to people who work with him, Mr Bilkey has taken some of the abuse heaped on DP World quite personally, as the controversy in the US has intensified. He identifies himself closely with Dubai and fails to understand the mistrust of his adopted home.

Ever the pragmatist ("I always try to make lemonade out of lemons," he quips), he is determined to turn some of that criticism on its head, citing the company's excellent record - it was last week named terminal operator of the year at awards in London hosted by Lloyd's List, the shipping newspaper. He will argue that DP World is prepared to become a world leader in improving container port security.

However, he will come up against not only the US national politicians who have heaped abuse on DP World but also a series of local US port authorities run by political appointees who may see both a political and a commercial reason to try to terminate P&O's terminal leases with the change in control. It might prove possible to re-let the leases to other operators on more advantageous terms.

Mr Bilkey, however, sees no reason at all why DP World should not be at least as good a ports operator as was P&O. He also has a powerful understanding both of US ports and of the politics of some of the places where the company could face the most severe problems. His family were powerful local politicians in New Jersey, whose governor, Jon Corzine, has vowed to end DP World's half-ownership of the company that operates Port Newark Container Terminal.

Mr Bilkey, who has postponed his planned retirement to see through the P&O deal, is likely to see such opposition as merely the latest challenge in a long career of overcoming such hurdles. Only the very bold would predict success for his opponents.

***

EDITORIAL: Ports in a storm
21 February 2006
The Baltimore Sun

Until last week, the fact that a foreign company, Peninsular & Oriental Steam Navigation Co., manages the loading and unloading of cargo in Baltimore and five other U.S. ports didn't seem particularly noteworthy. But the impending takeover of the London-based company by Dubai Ports World has changed all that. Because DPW is owned by the United Arab Emirates, a country that was used as a staging point for the 9/11 hijackers, the potential security ramifications have suddenly become a hot issue. P&O has a presence in 100 ports around the world. Now the question is whether Baltimore's port (or any of the others) will be put at risk when the company is run by Dubai Ports World.

Rep. Peter T. King, a Republican who chairs the House Homeland Security Committee, is concerned about potential infiltration of DPW by terrorists. And in recent days, numerous Democrats, including Maryland's Rep. C. A. Dutch Ruppersberger and Mayor Martin O'Malley, have raised similar concerns. The Bush administration hasn't done much of a job explaining its position: Homeland Security Secretary Michael Chertoff says security issues have been reviewed and certain requirements have been put in place, but he has declined to indicate what those requirements are publicly because that information is classified.

Potentially lost in this uproar is a clear understanding of what a stevedoring firm such as P&O does. For the record, its employees do not touch cargo. They aren't in charge of port security. They do not oversee shipping manifests. Stevedores are the middle managers who tell longshoremen when and where to load and unload cargo. That's pretty much it. In Baltimore, P&O employees are local people, most with extensive port experience, who help manage container operations at the Seagirt and, to a lesser extent, Dundalk marine terminals.

That's not to suggest that port security is not a legitimate issue. It is. Since 9/11, the Bush administration has paid far too little attention to this potential threat to the nation. There's a danger someone will try to use a container to smuggle a weapon of mass destruction into the country, for instance. But exactly how a stevedore could facilitate such an act is not entirely clear. The fact that most cargo is never inspected by a government official after it arrives at a U.S. port would seem like a more troubling vulnerability, but nobody's talking about that.

In this post-9/11 world, it's not hard to scare the American people, and Democrats are understandably frustrated that Republicans are seen as the party that's tougher on terrorism. But the recent criticism of the $6.8 billion P&O deal seems more than a bit over the top. Congress may deserve better answers than Mr. Chertoff has provided, but little revealed about the deal so far suggests it deserves to be torpedoed.

END

03/09/2006 16:40 FAX 202 226 2524 CG&MT SUBCOMMITTE 002

For the Record
CG&MT Hrg 3-9-06

STATEMENT OF THE HONORABLE DON YOUNG, CHAIRMAN TRANSPORTATION AND INFRASTRUCTURE COMMITTEE AT THE COAST GUARD AND MARITIME TRANSPORTATION SUBCOMMITTEE HEARING MARCH 9, 2006

FOREIGN OPERATIONS OF U.S. PORT FACILITIES

RECENTLY, A COMPANY BASED IN THE UNITED ARAB EMERITES AND OWNED BY THAT GOVERNMENT, DP WORLD, HAS AQUIRED A BRITISH COMPANY, P&O PORTS.

THIS PURCHASE HAS FOCUSED THE ATTENTION OF THE PEOPLE OF THE UNITED STATES ON THE SECURITY OF OUR PORTS.

MANY PEOPLE ARE UNAWARE THAT FOREIGN COMPANIES OPERATE CERTAIN PORT FACILITIES IN THIS COUNTRY AND ARE CONCERNED ABOUT THE RISK TO OUR NATIONAL SECURITY.

THE AMERICAN PEOPLE HAVE PLACED THEIR TRUST IN US THAT WE WILL ENSURE THE SAFETY, SECURITY, AND EFFICIENCY OF OUR PORTS, AND WE MUST NOT DISAPPOINT THEM.

AFTER THE EVENTS OF SEPTEMBER 11, 2001, OUR AWARENESS OF THIS TRUST COMPELLED US TO CREATE THE MARITIME TRANSPORTATION SECURITY ACT OF 2002, TO PREVENT TERRORIST ATTACKS AT OUR PORTS.

THIS HEARING WILL EXPLORE HOW THE OPERATION OF U.S. PORT FACILITIES BY FOREIGN COMPANIES COULD AFFECT THE IMPLIMENTATION OF THAT STATUTE AND THE SAFETY AND SECURITY OF U.S. PORTS.

IT WILL COVER PORT SECURITY FACILITY PLANS, CARGO SECURITY, AND THE IMPORTANCE OF FINISHING THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIALS, AN ID CARD THAT HAS BEEN DELAYED FOR FAR TOO LONG.

I LOOK FORWARD TO HEARING FROM THE WITNESSES.

Shirley, Gilda

From: Canter, Marsha
Sent: Tuesday, March 14, 2006 12:19 PM
To: Hewett, Christopher; Shirley, Gilda
Subject: Tay's Testimony - final (2)

Can you please put this in the record for our CG&MT subcommittee hearing that was held on 3/9/06? Thanks.

Introduction ... Who is NAWE?

Good afternoon, I'm Tay Yoshitani, the Senior Policy Advisor to the National Association of Waterfront Employers (NAWE), a national trade association which includes most of the large private sector marine terminal operators in the U.S. Briefly by way of background, prior to this role with NAWE, I served as Executive Director at both the Port of Oakland and Baltimore, and was the Deputy at the Port of Los Angeles (bio attached). On behalf of NAWE, I want to thank the members of the Senate Committee on Commerce, Science and Transportation for giving us the opportunity to comment on maritime cargo security and S. 1052.

NAWE members work closely with port authorities, ocean carriers, railroad and trucking companies, organized labor and shippers to ensure the smooth flow of international commerce that keeps our country's economy strong. It is estimated that the maritime industry handles about 15% of the U.S. GDP. Our membership reflects the international scope of the maritime industry and terminal operations. Many of the members are U.S. company-owned, but many are foreign-company owned as well. In fact, P&O Ports has long been an active member of NAWE and holds a seat on the Board of Directors.

NAWE has been involved with port security since concerns were first raised almost 10 years ago. This Association testified before this Committee on the initial Maritime Transportation Security Act (MTSA) several months before 9/11, and, since its passage, we have been involved with the Coast Guard, TSA, CBP, and other elements of DHS as MTSA-based security regulations, C-TPAT, and cargo inspection programs have been developed and implemented.

What Do Terminal Operators Do?

Recent events have brought much attention on the typical structure of most U.S. ports and what role terminal operators play. As you know, the vast majority of ports in the U.S. are publicly owned by a state or municipal authority. Typically, the port authority, as land and fixed asset owner, leases out

marine terminals to terminal operators but retains a multitude of important responsibilities. As terminal operators, our members typically lease property from ports and essentially conduct the business of loading and unloading cargo between ships and marine terminals. This sounds a bit simplistic, but it's not. On any given day, there may be several ships at berth with thousands of containers being loaded and unloaded, while a comparable number of trucks are entering and exiting our terminal to pick up or drop off a load. To do this day-in and day-out in a safe manner, while keeping track of where each container is and where it is supposed to go, is a daunting task.

It is worth noting that some terminal operators provide a service that is more limited in scope than what I have just described. For example, in some cases, private operators are pure stevedores, servicing terminals run by operating port authorities. Regardless of scope, we conduct our business in compliance with numerous federal statutes, regulations and policies. In this post 9/11 world, many of these are, of course, security related. In fact, we are perhaps one of the most federally regulated industries in the country.

What is a Terminal Operator's Role in Port and Cargo Chain Security?

Given recent interest in the role of marine terminal operators, I want to take a moment to clarify how we view our role, specifically with respect to port and cargo security. To do this, it's helpful to separate security issues into basically two categories. The first is "facility security" which includes the port in general and individual marine terminals. The MTSA clearly designates the Coast Guard as the lead authority on port facility security. Under Coast Guard regulations, terminal operators are required to submit a comprehensive Facility Security Plan (FSP) for approval. Subsequent to initial submission, the Coast Guard conducts regular audits as well as annual exercises. Terminal operators are well aware that failure to comply with this approved plan may be cause for closure of the facility. Needless to say, terminal operators take these plans, audits, and exercises very seriously.

In conjunction with the Coast Guard, the Port Authorities are also actively engaged in facility security matters. Many Port Authorities have their own Port Police Force while others have a contractual relationship with their respective municipal police authority. A typical lease between the port and terminal operator may include security requirements that are borne by the lessee. But ultimately, the terminal operator is responsible directly to the Coast Guard on terminal security matters.

One key aspect of facilities security is access control of people and equipment. NAWE is in strong support of the upcoming TWIC program. We have reached out on a number of occasions to both the Coast Guard and TSA regarding this program including a recent submission of a "white paper" (see Attachment A) that includes recommendations with respect to truck gates at marine terminals.

The second area of security is what we refer to as the "cargo chain." Essentially, this refers to understanding "what is inside the container." Much has been written about this aspect of security, and it is the area of risk that most concerns those who understand maritime industry. The terminal operator actually has very little to do with this aspect of security other than a supporting role of moving containers around under the direction of CBP/DHS. When CBP wishes to inspect a container, they notify the terminal operator of the box number only. They do not reveal the name of the shipper, content, origin, or destination.

The "business service" that terminal operators provide is measured in terms of the "container unit." We need to know from the customer what the disposition of the container should be. Is it for pick-up by a local business by a trucking company? Is it to go to a nearby rail yard for transport to some inland destination? For our purposes, we don't have a business interest in knowing the content of the container. We are not given this information and we do not track this information. The one exception is if there is hazardous cargo in a container. We would know this because it is included in the ocean carrier's stowage plan, and these containers require special handling by the terminal operator. Of course, we are well aware that regulations are being drafted for "cargo chain security" as we speak. Although terminal operators will have no responsibility for cargo within containers, these impending regulations may call for the terminal operator to play some role in making sure that container seals have not been breached. But here again, we anticipate that our role would be limited to reporting the breach to the proper authority and taking action only under that authority's direction.

We recognize that security is everyone's business and requires a public-private partnership. NAWE and all of its members have been working closely with our partners at the Coast Guard, Transportation Security Administration, and Customs and Border Protection. We were active members of the MTSA Subcommittee of the Commercial Operations Advisory Committee. We are currently involved in the ISO RFID electronic seals discussion that may ultimately establish the much needed standard for the industry. And, it is worthy to note that all of our members are C-TPAT compliant.

NAWE Perspective on Maritime Security Concept/Approach

NAWE is in full support and agreement with the approach that the public-private partnership is taking to address maritime facilities and cargo chain security.

1. The "layered approach" is rational and makes good sense. No system by itself will ever be perfect. It makes sense that the initial layers begin well before the container reaches our terminals. After screening and targeting, the 24-hour rule permits CBP to get manifest data before loading at the foreign port. CSI allows comprehensive vetting before vessel loading.

And, finally, before reaching our terminals, the Coast Guard has the option to board a vessel before it enters our harbors. The layered approach minimizes the chance of a breach of the system.

2. "Risk mitigation" is also a critical element of the approach. This starts with risk assessment one container at a time. CBP must be able to narrow their focus and direct their attention to a manageable percentage of containers in order to physically inspect them.
3. "Pushing the borders out" is also an excellent approach for inbound cargo and goes hand-in-hand with the "layered approach." The CSI program and RPMs at foreign ports are examples of pushing the borders out. There are other developments such as the Integrated Container Inspection System (ICIS), thought not yet fully tested, that hold promise of further strengthening this approach. The detection of problem containers needs to be well before they reach our terminals. The focus must be at the point of stuffing the container and loading on to a ship.

4. Controlling access to marine terminals using the impending TWIC program is also a good approach. However, at this point, it is our understanding that technology problems still exist with scanning of cards and biometric indicators. The accuracy rate of the TWIC system must be very high for the system to be effective. Subject to resolution of these problems, we are in strong support of this program and continue to urge early implementation.

5. We all recognize that this is an international business and security issues transcend international borders. Therefore, our solutions must be implemented with international cooperation. International standards must be agreed upon before various security programs can be implemented on a global basis.

6. And lastly, leveraging appropriate technology makes a lot of sense. Terminal operators are already employing various technologies such as OCR and RFID to not only improve operations but enhance security as well. We support the use of technologies as long as they are appropriate and fully tested.

We support all of these concepts/approaches. If all of these approaches could be fully implemented, overall security at the facilities and the cargo chain would be greatly enhanced.

Comments on S. 1052

We have reviewed the "Transportation Security Act" (S. 1052) using the six approaches and concepts that I just mentioned and find them to be consistent. Therefore, NAWE fully supports this Senate bill as currently written. In the interest of time, I wish to limit my comments to three key points. However, we would be happy to submit, in writing, responses to any questions you might have on any of the specific provisions of this bill.

1. Provisions indicate clear recognition that DHS must obtain more and better information about what is being loaded inside the container at the point of "stuffing." This is followed by the upgrading of our Automated Targeting System. We believe this represents the most significant opportunity to improve cargo chain security. We are encouraged that this bill would do much to improve upon this critical area.

2. The CSI program is perhaps the most important effort to "push the borders out." This bill includes provisions to continue and enhance this program. This program needs to be adequately funded and expanded as quickly as possible.

3. And, lastly, I'll just mention that we are encouraged that leveraging technology is an important element of this bill. The number of containers entering and leaving the U.S. is expected to grow rapidly over the next couple of decades. There is no way that facility and cargo chain security can be significantly enhanced without advances in technology.

What Else Should DHS and Their Agencies Be Doing?

In conclusion, NAWE is in support of the overall approach that is being taken to improve maritime facilities and cargo chain security. We also support S. 1052. We understand and recognize that terminal operators do have an important role in this public-private partnership. We stand ready to do our part.

We are concerned about the pace at which progress is being made on the various fronts. Cargo chain security regulations and the TWIC program are two that come to mind. Both of these are complex, but they are vital to upgrading facility and cargo chain security. Proposed regulations should be issued as soon as possible. And we urge this Committee to continue to provide the resources and oversight to bring these programs to completion. Along with all our colleagues in this industry, members of NAWE have a direct and vested interest in overall maritime security. In this regard, NAWE has, in the past, offered to provide a "loaned executive" to both the Coast Guard and the TSA to provide industry expertise. We are respectful of the established rule making procedures but continue to stand by this offer.

My last note is to invite all members of this Senate Committee and members of your staff to visit

one or more of our members' terminals. I can promise you that it will be interesting and well worth the investment of your time. Please feel free to contact me or any of my colleagues at NAWE to coordinate a tour at a terminal that is convenient to you. I can assure you that our members would be delighted and honored to host a tour.

Again, thank you for the opportunity to address this Committee. I'd be happy to answer any questions you might have at the appropriate time.

3/17/2006

○